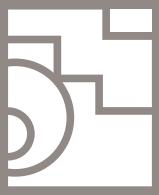


Universities UK

Oversight of security-sensitive research material in UK universities: guidance

October 2012

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 authors in danger of arrest and prosecution under, for example, counter-terrorism legislation. Certain procedures for independently registering and storing this material – through research ethics processes – are recommended in this guidance.

Recommendations

Security-sensitive research in UK universities requires the expansion of existing research ethics approval processes. This might involve new online questionnaires for researchers at universities.

Security-sensitive research material that can be interpreted as engaging Terrorism Act (2006) provisions should be kept off personal computers and 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, but 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 started for ethics officers (or their counterparts) and IT officers in universities in implementing the ethics review process and secure storage of sensitive material.

1 Background

This guidance has been developed following (i) ongoing discussions among stakeholders in security research in the UK that have been active since 2008; and (ii) the Universities UK report *Freedom of speech on campus: rights and responsibilities in UK universities* (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, who has taken part in stakeholder discussions, was commissioned to write this guidance in consultation with the higher education sector.

2 Scope of the guidance

This guidance:

- outlines specific ethical issues arising in this area and gives a template for a questionnaire which 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) adapting or applying the model

3 Security-sensitive material: the issues

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. At least one researcher, in Italy, conducts his research into jihadist activity by impersonating a jihadist in internet chat rooms used by

extremists.[1] He does so conscious of the fact that his behaviour may come to the notice of Italian counter-terrorism police.[2]

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 Ministry of Defence-commissioned work on military equipment, 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 A mechanism for 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 at preventing 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

[1] The researcher in question disclosed this at an international terrorism conference held in London by the Royal United Services Institute for Defence and Security Studies on 2 and 3 October 2008.

[2] Personal communication, December 2008

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[3] or suitable counterparts in universities without ethics officers (eg, 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 required at the moment in some universities. For example, at the University of Birmingham, postgraduate research projects that involve terrorism-related material not only have to be disclosed to the university, they also have to be vouched for by the heads of the relevant departments.

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.

Sections 2 and 3 of chapter 11 of the Terrorism Act (2006) 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 endorsing or promoting terrorism. A summary of these sections might 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 document titles on the server and 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.

[3] Normally the academic chairs of research ethics committees, as opposed to administrative staff connected to research ethics committees.

4.1 Items in the safe store

A store of security-sensitive material on a university server will mainly contain documents that, like 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 not only contain 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 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

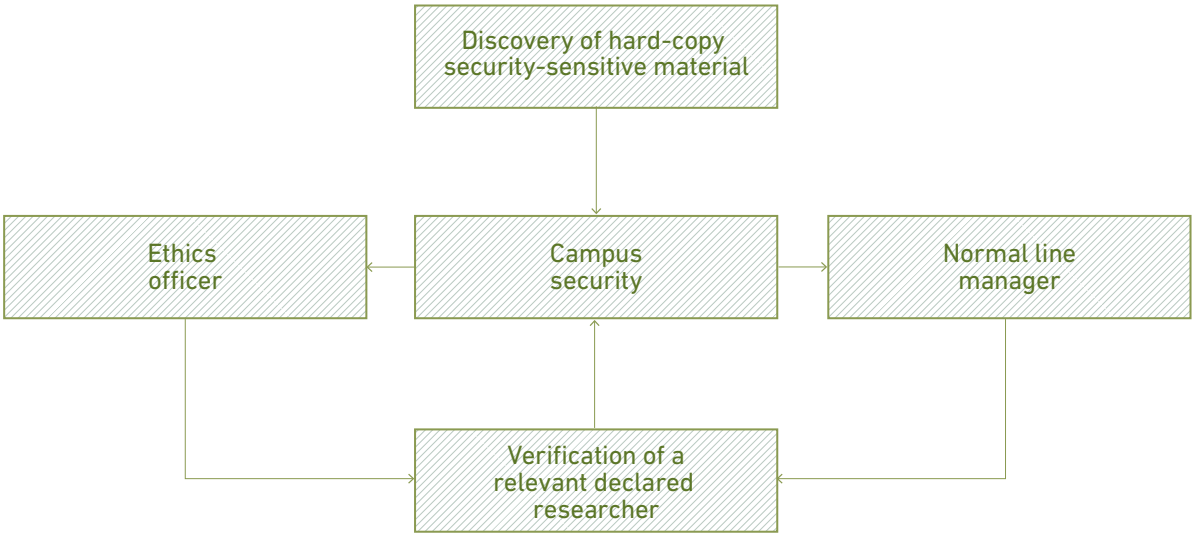
Ethics officers or their counterparts would know who was carrying out declared security-sensitive research in a university, and so would be in a position to confirm whether or not an individual found to possess such material was a declared researcher with a good reason for using it. On the other hand, ethics officers would not know what the research content was in any detail, and would not communicate about even 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. But 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 individual university policy, ethics officers or their counterparts would be first or early points of contact for both internal and external enquiries about discovered research-sensitive material.

4.2.1 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, though 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, themselves previously briefed about the policy on security-sensitive material, who could then contact their normal line manager and the ethics officer for verification of a relevant declared researcher (Figure 1).

Figure 1: internal enquiries

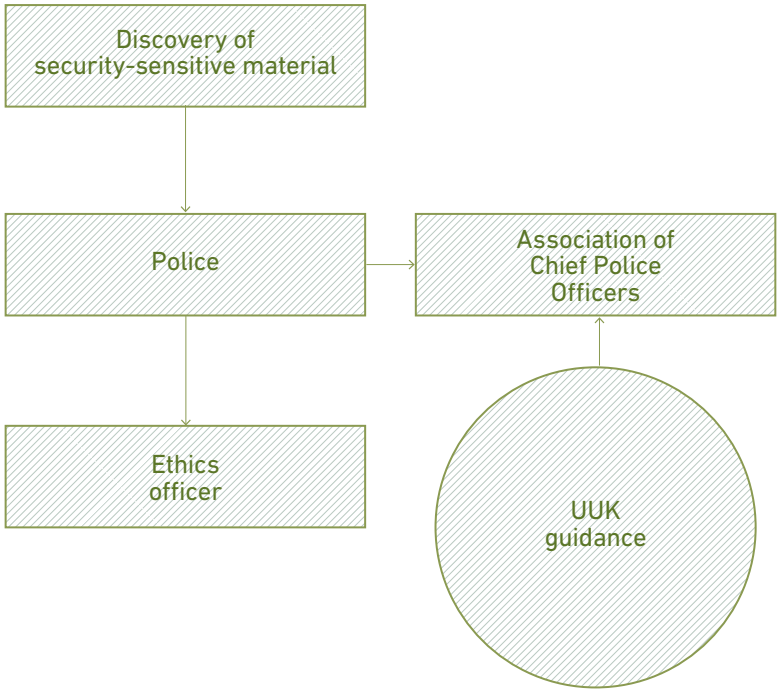


4.2.2 External enquiries

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 (see Figure 2). 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[4] – this should form part of routine engagement with the police on campus safety and crime prevention. Properly briefed in this way, the police are likely to treat suspect university-associated material as innocent until proven otherwise.

[4] See 2008 ACPO guidelines on the application of neighbourhood policy to higher education institutions.

Figure 2: external enquiries



University ethics offices 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.[5]

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,[6] and work in many or most universities. This makes it straightforward to offer them training on a national basis in security-sensitive research

[5] 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.

[6] 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. I am grateful to Dr Brendan Laverty of the Research and Commercial Services Department at the University of Birmingham for information about AREC.

issues, and to roll out a system of oversight of such research in most UK universities.

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 was 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 foolproof, 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 everyone 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.

Do the proposed mechanisms single out Muslims? 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), whether that terrorism is Muslim-linked or not. 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 IT

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. A training programme should include:

1. a review of current terrorism legislation relevant to research
2. suggested contents for forms (electronic and paper) for an ethics approval process
3. suggested internet user advice
4. what secure server contents would look like when accessed by an ethics officer
5. what secure server contents would look like when accessed by a researcher
6. what ethics officers should do in the case of a query about security-sensitive research material from within their university
7. what ethics officers should do in the case of a query from outside their university

The training would probably also involve information for IT officers about the hardware and software necessary for a secure, central storage system.

ANNEXE A

Template for general online questions on security-sensitive material

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

a. commissioned by the military:

Yes	No

b. commissioned under an EU security call:

Yes	No

c. involve the acquisition of security clearances:

Yes	No

d. concerns terrorist or extreme groups:

Yes	No

If your answer to question 1d 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 promoting or endorsing terrorist acts.

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 questions 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 document store:

Yes

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

Yes	No

5. If you answer '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 putting an 'X' in the 'Yes' box.

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 document store. These titles will only be available to the ethics office. Please acknowledge that you accept this by putting an 'X' in the 'Yes' box.

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 terrorist acts, even terrorist acts carried out in the past. 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 and downloading of material issued by jihadist 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 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 security offices

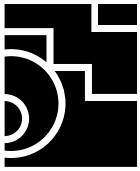
Some university research involves the use of security-sensitive material, including material related to terrorism and extremism. Procedures exist for storing this material and not circulating it if it is being used for legitimate research purposes. If such material is handed in, please inform _____ and the research ethics officer.

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.



Universities UK

Universities UK (UUK) is the representative organisation for the UK's universities. Founded in 1918, its mission is to be the definitive voice for all universities in the UK, providing high quality leadership and support to its members to promote a successful and diverse higher education sector. With 134 members and offices in London, Cardiff and Edinburgh, it promotes the strength and success of UK universities nationally and internationally.

Universities UK
Woburn House, 20 Tavistock Square, London, WC1H 9HQ

Tel +44 (0)20 7419 4111

Email: info@universitiesuk.ac.uk
Website: www.universitiesuk.ac.uk
Twitter: @UniversitiesUK

ISBN: 978-1-84036-275-6

October 2012