# 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 VHFWLRQ RI WKH 7HUURULVP $FW DQG WKH 7HUURULVP $FW academic research purposes. Such security sensitive research material should therefore be kept off personal computers and stored instead on specially designated university servers VXSHUYLVHG E\ XQLYHUVLW\ HWKLFV RI¿FHUV RU WKHLU FRXQWHU authorities. This material could be accessed easily and securely by researchers, and would not be transmitted or exchanged.

- (WKLFV RI¿FHUV RU WKHLU FRXQWHUSDUWV VKRXOG EH D ¿UVW RU HDUO\ SRLQ 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 WUHDWHG DV KDYLQJ D OHJLWLPDWH UHVHDUFK SXUSRVH XQOHVV 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 XVHUV 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 o IIHUHG WR HWKLFV RI¿FHUV RU WKHLU FRXQ , 7 RI¿FHUV 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.

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 definit
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 issu
al-Qaeda manual, for example, can be highly relevant to many kinds of perfectly legitimate academic research – studies of jihadism international relations
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

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

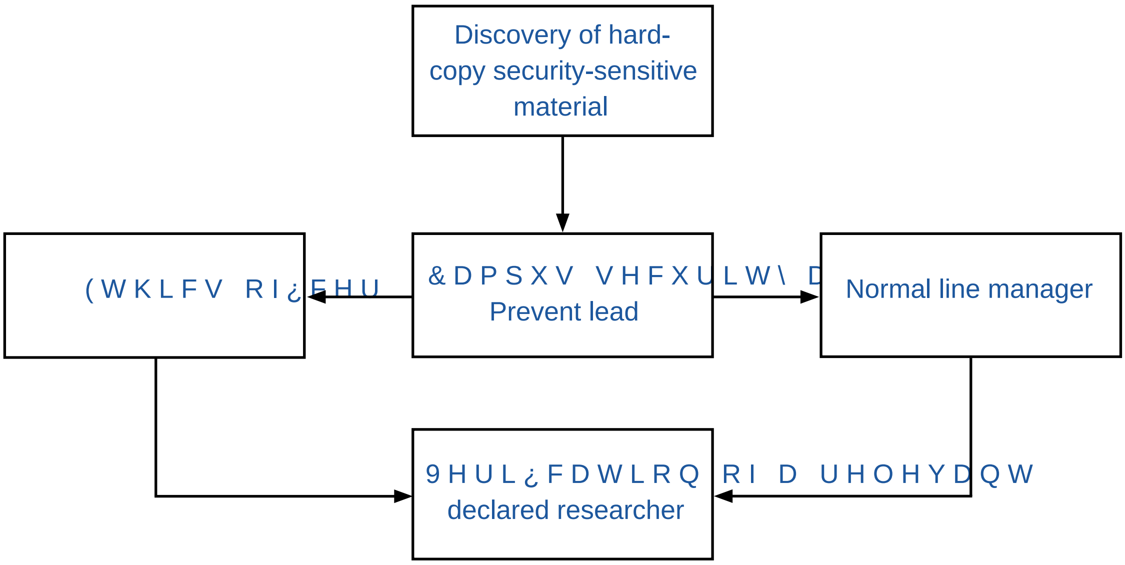
(WKLFV RI¿FHUV RU WKHLU FRXQWHUSDUWV ZRXOG NQRZ ZKR ZDV FD
UHVHDUFK LQ D XQLYHUVLW\ DQG VR ZRXOG EH LQ D SRVLWLRQ WR
WR SRVVHVV VXFK PDWHULDO ZDV D GHFODUHG UHVHDUFKHU ZLWK D
KDQG HWKLFV RI¿FHUV ZRXOG QRW NQRZ ZKDW WKH UHVHDUFK FRQ
FRPPXQLFDWH HYHQ WKH WLWOHV RI VWRUHG GRFXPHQWV XQOHVV

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
EH DW RQH UHPRYH IURP HWKLFV RI¿FHUV RU WKHLU FRXQWHUSDUW
RI¿FHUV RI GHFODUHG UHVHDUFKHU VWDWXV ZRXOG EH HQRXJK WR
RI PDWHULDO ZDV OHJLWLPDWH DQG QRW WR EH LQWHUIHUHG ZLWK
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
LQWUXVLRQ HWKLFV RI¿FHUV DQG KHDGV RI GHSDUWPHQW 'HSHQGL
XQLYHUVLW\ HWKLFV RI¿FHUV RU WKHLU FRXQWHUSDUWV ZRXOG EH
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
RI WKLV NLQG VKRXOG ¿UVW EH WDNHQ WR FDPSXV VHFXULW\ DQG R
briefed about the policy on security-sensitive material, who could then contact his or her normal line
PDQDJHU DQG WKH HWKLFV RI¿FH IRU YHUL¿FDWLRQ RI D UHOHYDQ

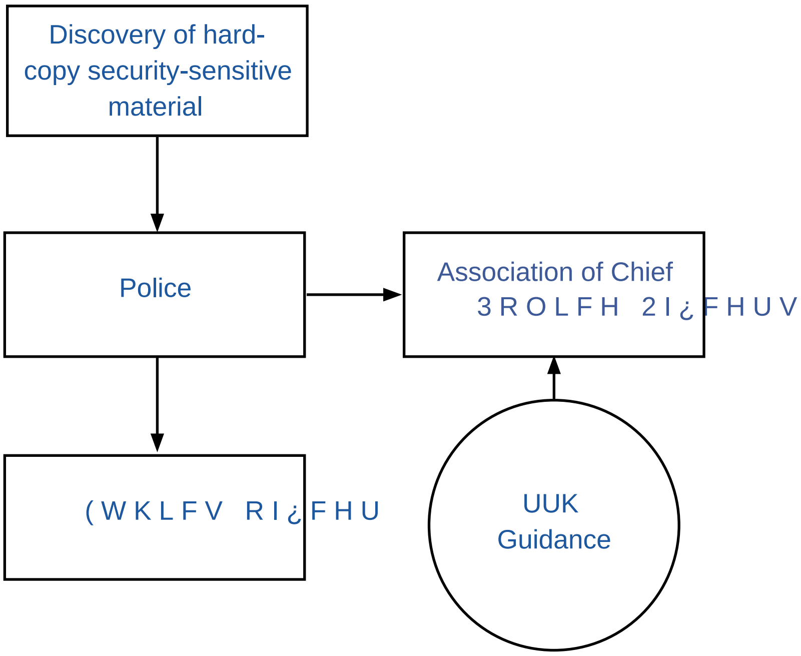
## FIGURE 1: INTERNAL ENQUIRIES


Discovery of hard-copy security-sensitive material
&DPSXV VHFXULW\ D Prevent lead
(WKLFV RI¿FHU
Normal line manager
9HUL¿FDWLRQ RI D UHOHYDQW declared researcher

## 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 WKH HWKLFV RI¿FHU RI WKH XQLYHUVLW\ FRQFHUQHG )LJXUH LQ It would aid this approach if universities were to share their procedures in this regard with the local SROLFH DQG SURYLGH D ¿UVW SRLQW RI FRQWDFW ± WKLV VKRXOG I SROLFH RQ FDPSXV VDIHW\ DQG FULPH SUHYHQWLRQ $VVRFLDWLRQ Properly briefed in this way, the police are likely to treat suspect university-associated material as innocent until proven otherwise.

## FIGURE 2: EXTERNAL ENQUIRIES


Discovery of hard-copy security-sensitive material
Police
Association of Chief 3ROLFH 2I¿FHUV
(WKLFV RI¿FHU
UUK Guidance

8QLYHUVLW\ HWKLFV RI¿FHUV WKHPVHOYHV PLJKW RIIHU ERWK YRLFH 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 XQLYHUVLW\ UHVHDUFK LQ WKH 8. EXW HWKLFV RI¿FHUV DUH FUHGL FUHGLEOH FXVWRGLDQV RI XQLYHUVLW\ UHVHDUFK VWRUHV (WKLFV KHDG UHVHDUFK HWKLFV FRPPLWWHHV ± RU WKHLU FRXQWHUSDUWV universities for enquiries about security-sensitive material discovered on university computers. Ethics RI¿FHUV KDYH QHWZRUNV WK[4] DW H[WHQG DFURVV WKH 8. 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 UHFRUG 'UDIW UHVSRQVHV ZRXOG EH FRSLHG WR D UHJLVWUDU DQG RU SUR YLFH FK EHLQJ DXWKRULVHG IRU UHOHDVH WR WKH HQTXLUHU )XOOHU SROLFH HQTXLULHV ZR 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
WR D UHVHDUFK HWKLFV SURFHVV RU FKHFNV E\ DQ HWKLFV RI¿FHU

7KH ULJKW UHVSRQVH WR WKH GDQJHU RI RI¿FLDO PLVLQWHUSUHWD
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
LQ D JLYHQ XQLYHUVLW\ 2QFH DJDLQ WKH PHVVDJH VHQW RXW IUR
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-
VHQVLWLYH PDWHULDO DQG DERXW WKH VKHHU EUHDGWK RI WKH O
effect of encouraging terrorism (see Annexe B), concerns all or most people in universities, and not just researchers.

%\ SURYLGLQJ FOHDU DGYLFH DQG UHVHDUFK VSHFL¿F PHFKDQLVPV
GLI¿FXOWLHV DULVLQJ IURP LQGLYLGXDOV DFFHVVLQJ VHQVLWLYH P

## 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.

'R WKH SURSRVHG PHFKDQLVPV VLQJOH RXW VSHFL¿F JURXSV" 1R 7
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
VHFXULW\ VHQVLWLYH PDWHULDO ZLOO QRW VWLJPDWLVH DQ\ VSHFL

# 7. ETHICS OFFICERS AND INFORMATION TECHNOLOG COLLEAGUES

Since the mechanism suggested in section 4 of this guidance involves a secure server, it will carry
VRPH DGPLQLVWUDWLYH DQG PRQHWDU\ FRVWV WR XQLYHUVLWLHV

# ANNEXE A: TEMPLATE FOR GENERAL QUESTIONNAIR SECURITY-SENSITIVE MATERIAL

'RHV \RXU UHVHDUFK ¿W LQWR DQ\ RI WKH IROORZLQJ VHFXULW\ VHQ
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 ETHIC 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

# ANNEXE C: ADVIC2T2NctipaTERNET USE FRADOM50.1

# 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 UHVHDUFK SXUSRVHV ,I \RX FRPH DFURVV PDWHULDO WKDW VHHPV W DWWHQWLRQ RI WKH XQLYHUVLW\ VHFXULW\ RI¿FH

## 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 _______________________________* DQG WKH UHVHDUFK HWKLFV RI¿FHU

*Insert name

# ANNEXE E: ONLINE FORM FOR ETHICS OFFICE SECUR 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 RI¿FH FDUULHV RXW FKHFNV UHOHYDQW WR HVWDEOLVKLQJ ZKHWKH

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

7KDQN \RX 7KLV RI¿FH ZLOO FRQWDFW \RX DQG XQGHUWDNH DQ LQY

# REFERENCES

$&32 3UHYHQW 3ROLFH DQG 8QLYHUVLWLHV DYDLODEOH DW ZZ
XSORDGV ¿OHV WDPSUHYHQWSDQGXQLJXL SGI

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.