Guidance Note: The oversight of security-sensitive research

May 2016

What is this about?
The possession or distribution of sensitive material by researchers can be open to misinterpretation by law enforcement authorities, and can put academics in danger of arrest and prosecution under counter-terrorism legislation.
This document provides guidance on the safe management of security-sensitive research material. It explains what constitutes security sensitive research material and provides a framework for its secure management, including open declaration, ethical scrutiny, safe keeping and secure disposal. The framework is designed to protect research staff and students from any misunderstandings and/or false accusations relating to the possession or use of this material.

Who is this guidance aimed at?
This guidance is intended for all staff and students of the University who engage in or supervise security-sensitive research.

How does the University monitor compliance with this guidance?
This guidance will be reviewed annually to ensure its on-going effectiveness.

If you have any queries about this guidance, please contact:

The University Ethics Adviser simon.kolstoe@port.ac.uk
or the Research Governance Manager denise.teasdale@port.ac.uk

1.0 Introduction

Universities play a vital role in carrying out research on issues where access to, or possession of ‘security-sensitive material’ is necessary. All security-sensitive material must be managed carefully and securely to avoid any misunderstandings and/or false accusations relating to the possession or use of this material.

2.0 Scope of the document

This document outlines the issues arising from security sensitive research and sets out a framework designed to protect legitimate researchers. **Following the**

framework can significantly reduce the legal risks arising from legitimate research involving security sensitive material. However, the framework cannot guarantee immunity from prosecution under the law.

3.0 What is 'security-sensitive research material' ?

3.1 The possession or dissemination of security sensitive research material could be considered unlawful under the terms of The Terrorism Act 2006 Chapter 11 (Part 1: Offences). Researchers are advised to study this legislation before engaging in research which relies on the need to access or store this type of material.
In outline, security sensitive research material includes, but is not limited to:

- Military or paramilitary training manuals or procedures.
- Documentation or media supporting extremist ideologies
- Instructions, guidance or advice on the planning or execution of terrorist acts.
- Instructions, guidance or advice relating to the acquisition or use of a radioactive device or radioactive material.
- Material supporting, inciting or condoning acts of terrorism
- Material intended to radicalise or proselytise individuals into adopting an extremist viewpoint.
- Material intended to recruit or otherwise enlist members or followers to banned organisations.
- Instructions, guidance or advice (including the acquisition of components) on the subjects of:
    - bomb making;
    - the manufacture of improvised explosive devices (IEDs);
    - the creation of chemical weapons or toxic agents;

Note: Information considered to be security sensitive research material is widely available on the internet and some material may also be available for access through the University Library. The legislation makes no distinction between sources so it is advisable to follow the framework irrespective of the source of the information.

3.2 Security sensitive research material may be highly relevant to many kinds of perfectly legitimate academic research. However, prosecutions under counter-terrorism legislation in the UK have been brought on the basis of an accumulation of downloaded material and other data, which is relevant to terrorist or extremist activities. It may 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 distribution, which might be conceived as terrorist purposes.

4.1 Framework for the secure management of security sensitive research

4.2 Open declaration

The ethical review questionnaire process includes an open declaration of research in security sensitive areas. 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.

4.3 What steps do I need to take to deal with this issue in my research?

If you suspect that your current or future research activities (including supervision of the research of others) might necessitate access to or downloading of, security sensitive material (as described in 3.0), then the following actions should be taken

1. Answer the general questions on security-sensitive research at Annex A
2. Complete the ethical approval form at Annex B
3. Submit the completed forms to your faculty ethics committee
4. **(If approval is granted)** Create a folder on your University Google Drive in which to store any downloaded security sensitive research material.

4.4 Rules for safe keeping security sensitive research material

4.3.1 Security sensitive research material must not be stored on a personal computer, USB device or external hard drive

4.3.2 Security sensitive research must only be kept in a dedicated folder on your University of Portsmouth GoogleApps account (your GoogleDrive).

4.3.3 The dedicated folder is a repository for security sensitive research material only. Research documents and other intellectual property related to or derived from the material must be stored elsewhere.

4.3.4 With the exception of the University Ethics Adviser and the University Research Governance Manager, this folder must not be shared with anyone else.

4.3.5 An index to the folder should also be created. This should provide a summary of the contents of the folder and a list of the titles it contains. This document should be shared with the University Research Governance Manager.

4.3.6 Security-sensitive research material material must not be transmitted to a third party or exchanged.

4.4 What oversight will be in place - for ethical scrutiny?
The University reserves the right to inspect the contents of the folder by ethics officers - at least every 6 months. Inspection could involve checking the folder contents against the index of titles or it could require direct access to file content.

4.5 How long can security sensitive research material stay on UoP storage?
This will be defined by the approved users and clearly set out in a terms of use agreement (see Annex F) when their account on safe store is created.

4.6 How should security sensitive research material be securely disposed of when no longer required?
In accordance with the terms of use agreement, data will be deleted on the date of expiry.

4.8 How would an access request from law enforcement be managed?
Any enquiry made to the University should first be directed to the Director of Corporate Governance University House, Winston Churchill Avenue, Portsmouth PO1 2UP (Tel (0)23 9284 8484)**. Subsequently, the Ethics Adviser or the Research Governance Manager would then be able to confirm (or otherwise) that the security sensitive material is being held for legitimate research purposes.**

ANNEX A General questions on security-sensitive research
Does your research fit into any of the following security-sensitive categories?
If so, indicate all which apply:

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 (Note 1:) ***If your answer is yes, go to the questions in Annex B.***	Yes	No

Note 1: What are terrorist or extreme groups?
Trying to define terrorism can be difficult and controversial, because so many people and countries see it differently. But any definition usually includes:

- *mass intimidation - trying to make lots of people scared to go about their everyday or normal life.*
- *unlawful violence or the threat of violence against the public*
- *violence intended to change a law, culture or political system, or to change how people think or act*

ANNEX B Ethical approval form (sensitive research)
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.	Yes No

	Access to this file store will be protected by a password unique to you.	
3a.	You agree to store all documents relevant to questions 1 and 2 on that file store:	Yes No
3b.	You agree not to transmit electronically to any third party documents in the document store:	Yes No
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 No
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 No
Countersigned by Ethics Committee Chair: Name: Signature:		

ANNEX 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.

ANNEX D Advice for individuals 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 the legitimate storage of this material and the prevention of its circulation. If you come across material that seems to fit this description, bring it to the attention of Campus Security (ext: 3418).

If such material is handed in, please inform the University Ethics Adviser simon.kolstoe@port.ac.uk and the Research Governance Manager denise.teasdale@port.ac.uk on ext 6191

ANNEX 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 / report	