Guidance policy for security sensitive material

1. What constitutes security sensitive material?

Security sensitive materials are defined here as materials that are covered by the Official Secrets Act 1989 and the Terrorism Act 2006, materials that could be considered 'extremist' according to the Counter Terrorism and Security Act 2015, defined as 'vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs', and materials that require security clearance before accessing. It should be noted that other material could be regarded as security sensitive, and, if in doubt, researchers should consult their Faculty Research Ethics Officer. Work commissioned by the Ministry of Defence is handled separately under MOD regulations. Staff and students conducting research involving security sensitive materials, and those affected indirectly by such research**,** are reminded that they should consider not only UK regulations but also the regulations from wherever in the world the research may be linked or carried out. Material could be in audio, visual and written formats and may include, but is not limited to; online, digital, electronic, telecommunication or hard copy sources.

2. The aims of this policy on security sensitive material

a. Oxford Brookes University is committed to providing an environment in which scholarly activity, including research and teaching, is encouraged and supported across the broadest range of subjects and disciplines. The University acknowledges the need to be vigilant in the management of security sensitive materials. The University takes seriously its responsibility to protect researchers from the misrepresentation of intent by authorities and to this end provides guidance in this policy document.

b. The University has a duty of care towards students, staff, contract researchers and the wider public with regard to research involving access to and/or storage of security sensitive material.

c. The University has drawn up this guidance policy in response to the requirement to clarify guidance for research involving security sensitive materials and has done so with reference to the Official Secrets Act 1989, the Terrorism Act (2006), and the Counter Terrorism and Security Act (2015).

d. This policy may be amended at such time as required on the agreement of the Chief Information Officer and the Pro Vice-Chancellor for Research and Global Partnerships.

3. To whom this policy applies

This policy applies to all students, both university and contract staff undertaking research and also any other scholarly activity such as teaching material development that may involve access to and use of security sensitive materials.

4. Mandatory Notification

a. The relevant Faculty staff, including subject specialists and the Faculty Research Ethics Officer will provide advice to individuals as to what type of material is 'security sensitive' and whether or not notification to UREC is required. Stages B to D are required for individuals who are engaging with materials deemed to be security sensitive.

b. Those who engage with security sensitive materials are required to notify, in writing at the outset of the work, the Head of Information Management or their nominated deputy, the relevant Faculty Research Ethics Officer and their Head of Department. A separate pro-forma will be completed as part of this process as retained evidence, and internal notification to the nominated Prevent Officer (Academic Registrar) is required.

c. Any individual undertaking research involving security sensitive topics and where the research also involves human participants is required to submit a full application to the University Research Ethics Committee.

d. Where research ethics approval is required and has been granted the relevant external security services, local or national will be informed by the UREC office where appropriate, before the commencement of the research.

5. Data issues

a. Security-sensitive materials should be collected and stored only with the knowledge and authorisation of the relevant university IT department (ITS). Access to the material should be by named individuals only and the Head of Information Management as authorised by the Chief Information Officer or their nominated deputy. Researchers/users should take into consideration the access, storage, transfer, publication, archiving, deletion and destruction of security sensitive data when designing and implementing their research.

b. Data can only be accessed, downloaded, and analysed on a dedicated, university provided encrypted laptop or a university provided secure virtual private network available through a secure lending service via IT Services. Personal devices must not be used for security sensitive materials. Further information is available from the relevant Faculty Research Ethics Officer, the nominated Prevent Officer (Academic Registrar) and the Postgraduate research supervisory team (if appropriate). Technical information is available from the Head of Information Management or their nominated deputy.

6. Risk Management

a. Any person engaging with security sensitive materials should be aware that such activity may result in adverse consequences that may be without time limitations or jurisdiction and these may be outside of the university's control.

b. Accessing security sensitive materials may result in the flagging of individuals by the security services which may impact upon their future ability to travel, job opportunities, their personal life and may also be extended to family members and those associated with the individual.

c. In some cases it is possible that prosecution by the authorities may occur as a result of the specific activities undertaken.

Approved by the University Research Ethics Committee 21 February 2016, revised and agreed on 21 September 2016

Approved by the Pro Vice-Chancellor, Research & Global Partnerships and the Director of Legal Services on 4 November 2016

Approved by the Prevent Duty Advisory Group on 11 July 2017

Approved by the University Research and Knowledge Exchange Committee on 26 September 2017

Approved by Academic Board on 8 November 2017

Approved by the Board of Governors on 21 November 2017

Security sensitive material notification

Please read the Guidance policy for security sensitive material and refer to the flowchart before completion.

The completed form should be submitted electronically either to the Chief Information Officer, IT Services, or attached to a full UREC application for research involving human participants. Include any other information specified in the guidelines for downloading security sensitive material.

Activity must not commence until the counter-signed form has been returned to you

Brief description of type of material to be accessed and for what purpose (maximum 150 words):

I the undersigned give notice of my intention to carry out teaching / research / attend a course (delete as appropriate) *relating to security sensitive material, which will potentially involve access to materials prohibited by law, during the period:*

From: _____ *until no later than:* _____

I agree to abide by the University Guidance policy for security sensitive material

I am aware of the University's Regulations relating to the use of Information Technology facilities (https://www.brookes.ac.uk/it/information-management/policies-procedures-legislation/) and will abide by them.

Name (block capitals) _____

Signature _____ Date _____

Countersignature*

Name _____

Signature _____ Date _____

* For staff this is the Head of Department, for Postgraduate research students this is the Director of Studies and for Undergraduate students this is the Faculty / Department Research Ethics Officer.

For IT Services use only

This is to acknowledge notification of the intention to carry out the specified activity relating to security sensitive material by the person named above for the defined period only.

Name _____

Signature _____

Security Sensitive Material
Completion of notification form

Please read the Guidance policy for security sensitive material before completion.