

UREC-SOP-001: Security Sensitive research and knowledge exchange (SSR & KE) activity

Version Number	1
Prepared by	Huzma Kelly (Research Ethics and Integrity Officer)
Reviewed by	Research Environment and Scholarly Communications Lead, RKEO
Approved by	University Research Ethics Committee (27 June 2023)
Effective Date	27 June 2023
Review Date	27 June 2024

Version Number	Edited by	Approved by	Effective date	Details of changes

1. Background

“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.**” [Oversight of Security Sensitive Research Materials in UK Universities: Guidance, Universities UK \(UUK\), 2019.](#)

UUK also states: 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.

2. Purpose

UUK 2019: 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. Please see the [University of Westminster Security Sensitive Research and KE Policy and Guidance](#) for information.

3. Procedure for Principal Investigators (PIs)

3.1. The PI must ascertain whether their research and KE activity is within security sensitive areas, they should do this by referring to the [University's Security Sensitive Research and Knowledge Exchange Policy](#), and discussing with their manager or head of school where they need advice. Taught course students must work closely with their supervisor, as should Doctoral Researchers with their Director of Studies/Supervisory team.

3.2. The PI must commence a VRE Research and KE Ethics Review Application form (known as the Ethics Application Form), which will further assist in ascertaining and recognising the types of potential harms of any research, including SSR & KE. The form contains questions around SSR & KE, and further guidance in completing these questions is available in the '[SSR & KE Guidance Note for Researchers](#)'.

3.3. Where security sensitive issues arise in the ethics proposal the Ethics Application Form must be submitted in the VRE promptly and directly to the University Research and Knowledge Exchange Ethics Committee (UREC). The research should be identified as Class 4 (*research which has significant ethical implications or the potential to cause a significant risk of harm, including research where there may be an institutional and/or reputational risk*). Note Class 4 **includes** security sensitive areas but is not limited to this either.

3.4. No research in the area of SSR & KE can commence prior to receiving ethics review with Approval or Approval with Conditions.

3.5. In the case of SSE & KE activity a completed risk assessment should be provided alongside the Ethics Application Form via the VRE. Advice regarding types of risks to consider can be gained by contacting UREC via research-ethics@westminster.ac.uk and shw@westminster.ac.uk

3.6. By submitting the Ethics Application Form within the VRE as Class 4, the VRE record acts as they University's register for SSR & KE proposals (confidential to the UREC Representatives i.e., Chair, Secretary, and also UREC members). All co-investigators and study team members should be listed and named in the Ethics Application Form and their roles clearly stated.

3.7. Where a researcher proposing to conduct security sensitive research and KE activity fails to submit an Ethics Application Form via the VRE for review to UREC, or where only a class 1 (self-assessment) VRE record exists, this would be considered a breach of the policy and the appropriate

process would not have been followed, whereby the University could confirm this research as legitimate.

4. Procedure for RECs (Research Ethics Committees)

4.1. If the PI submits an Ethics Application Form but does not identify any security sensitive issues where these may be found to exist, the receiving CREC must promptly and without delay progress the Form via the VRE only to UREC (**do not 'Request more information'**). The CREC representative must add a private VRE note, explaining the reason for the escalation and whom the escalation was made by i.e., identified by Chair or Secretary as potentially containing SSR & KE issues.

4.2. The receiving CREC may subsequently be consulted for advice by UREC, if needed, but the CREC must not carry out an ethics review (**or set Conditions**) but instead should progress the Form for review to the UREC. This is to ensure a sole review occurs.

4.3. Where an Ethics Application Form has been submitted (Class 2 or 3) and has not been correctly identified as Class 4 by a receiving REC, again, there would be a breach of the policy and failure to implement process correctly. Where this comes to light the research ethics approval (if given) would be suspended, and the research halted until mitigations are in place to address the policy implementation.

4.4. The UREC will consider the Ethics Application. This is because there is an inherent risk to the researcher and others they work with, in relation to potential infringement of the law or raising suspicions regarding illegal activity.

4.5. Where Approval or Approval with Conditions has been provided by the UREC, the VRE Application Reference Number and Application meta-data (i.e., proposal title, PI/Co-names, College) will be provided to the University Prevent Lead by the UREC Secretary. This is only for purposes of responding to enquiries re. the legitimacy of the research. The information will not be shared otherwise.

5. Accessing information or materials (PI and/or Named Study Team)

5.1. USBs or personal computers must not be used and only University servers should be used through your University user log-in credentials to access such material.

5.2. You must not transmit (email etc.) any material which is deemed security sensitive by the University even if it is publically available, and even not by means of secure transmission. Contravention of this would be deemed illegal.

6. Secure Storage

6.1. The UREC will provide guidance to the PI to acquire University secure storage for any material accessed and downloaded for secure restricted storage and access by the PI and any named study team members. No research or KE activity concerning SSR & KE material (including that publically available) can commence until such time as confirmation is provided by the PI to UREC that the secure store is available to use.

6.2. If no other conditions are remaining the UREC will provide an Approval letter and the research as outlined in the Ethics proposal (via the Research and KE Ethics Application Form) can commence. Any significant deviation from protocol may invalidate insurance and will invalidate approval from the University if it has not been provided to UREC as an 'amendment to protocol'.

6.3. No material contained in the secure store should be transmitted, including using encrypted and secure messaging services, provided by the University, to any third party, beyond the researchers specifically named on the Research Ethics Application Form. If a new researcher joins the team then this will require an 'amendment to protocol' to be submitted via the VRE to UREC. Similarly, if a researcher leaves or there is a change in PI, this must be reported to UREC via an 'amendment to protocol' also, immediately and before enacting any such changes on the ground, except in the case of an emergency.

6.4. Only the Prevent Lead via Information Systems and Services Team will have access to the secure store should it be required (see Section 5 below on instances where this may occur).

7. Enquiries from authorities or those working or studying at the University

7.1. The University will not report research and KE proposal titles or researchers' names relating to Security Sensitive Research and KE activity to anybody unless the information that such work is being carried out is already in the public domain such as the University staff profile web-pages. However, where the University is contacted by external authorities, such as the Police, to confirm whether such activity is legitimate research and KE activity, it will do so. This will be via the University's Prevent Lead in the first instance or the UREC Chair, if the Prevent Lead is not available at the time. The PI will be informed if this occurs.

7.2. On occasion the University Prevent Lead and UREC Chair may decide it is in the researchers' best interest to inform the Police or other security authorities of such research and KE activity during the ethics review stage or after a decision to Approve or Approve with Conditions is made, so that if any surveillance or suspicion does occur, then the authorities are already apprised that this is legitimate research which has also been registered (via the University's VRE) and/or approved by the UREC. Any contact with the authorities will be discussed in advance with the PI with the Prevent Lead and UREC Chair.

ENDS

PI Procedure

Ascertain whether their research and KE activity is within security sensitive areas

- Refer to the policy
- Discuss with manager/Head of school
- Work closely with supervisor or Director of Studies/Supervisory team

Initiate Ethics Application Form in the VRE

- The form contains questions around SSR & KE
- Further guidance: [SSR & KE Guidance Note for Researchers](#)

List all co-investigators and study team members in the Ethics Application Form and state their roles clearly

- Confidential to the UREC Representatives and members

- The research cannot start until the committee review with Approve or Approve with Conditions
- If the application has failed to be submitted for REC review or it's only class 1 (i.e. a self-assessment, Part A form), the University may not be able to confirm this research as legitimate.
- No research or KE activity concerning SSR & KE material (including that publicly available) can commence until PI has confirmed to UREC that the secure store is available to use.

If there is any change in PI, this must be reported to UREC via an 'amendment to protocol' in the VRE immediately and before enacting any such changes on the ground

Prepare and submit risk assessment with the Ethics Application Form in the VRE (**SEE SLIDE 2**)

- Advice regarding types of risks from:
- research-ethics@westminster.ac.uk
- shw@westminster.ac.uk

The application involving sensitive research and KE data will be submitted to the UREC as Class 4

- Class 4 includes security sensitive areas but is not limited to this either.

REC Procedure

