Approved Security Sensitive Research and Knowledge Exchange Activity Policy 2021/22

Version Number	1.1.
Prepared by	Huzma Kelly (Research Ethics and Integrity Officer)
Reviewed by	Research Committee (27 October 2021), Research Committee Chair's Action (21 January 2022)
Approved by	Research and Knowledge Exchange Steering Committee (7 February 2022)
Effective Date	7 February 2022
Review Date	6 February 2025

Version Number	Edited by	Approved by	Effective date	Details of changes

Contents

1. INTRODUCTION

The University supports vital research and KE activity into security sensitive areas and enables this to be carried out in line with current legislation. This policy is designed to protect researchers who are proposing to conduct legitimate research and knowledge exchange (KE) activity into security sensitive areas.

Universities UK's *Oversight of Security Sensitive Research Materials in UK universities* (2019) recognises 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". 1

The University enables and supports such research and KE activity to be carried out safely and with the mechanisms in place to allow such research to be recorded (i.e. registered internally and confidentially, via the Virtual Research Environment [VRE]), in case of enquiries from security services, police or other external authorities seeking confirmation that the work is actually legitimate and has undergone research and KE ethics review. Any material collected as a result of such legitimate research, even if already in the public domain, will only be kept securely with restricted access and not be transmitted to a third party.

A record of such research is not automatically or routinely provided to any authorities, but is available for access by the University's Prevent Lead or University Research and Knowledge Exchange Ethics Committee (UREC) Chair, should an enquiry be made by the authorities, internal colleagues or students, or a member of the public, should suspicions be raised by them regarding any activity or material related to the researcher(s)' work.

This policy covers research and knowledge exchange (KE) activities only, conducted by all researchers at the University, at all levels, including where the research or KE activity is led by another institution but includes a University of Westminster researcher contribution. It also covers Visiting Researchers as defined in the *Visiting Researchers Policy*. The policy covers research conducted in the UK and overseas. Where research is undertaken in overseas locations the researcher will also need to abide by local laws and regulations. This Policy still necessitates the need to meet other requirements for approvals which may be needed, including for work with ethical implications, governance requirements including legal and regulatory, as well as, specific safety, health and wellbeing requirements.

This policy is solely intended for the purposes of research and knowledge exchange activities. Those working in other areas should seek advice from their line manager or supervisor and continue to follow the University's *Information Systems Acceptable Use Policy (AUP).*

2. BACKGROUND

This policy is based on Universities UK's (UUK's) guidance (2019) relating to *Oversight of Security Sensitive Research Material at UK universities* as well as the statutory guidance from the Home Office; *Prevent duty guidance: for higher education institutions in England and Wales* (updated April 2021).

The UUK recognises that universities carry out a crucial and vital role in undertaking research in areas related to security, terrorism and resilience. It also acknowledges that such research requires particular care to be taken to avoid infringement of the law. Such work can be subject to surveillance and subsequent enquiries or investigations from security services, police or other authorities.

The policy is designed to enable the research and KE activity to be undertaken where processes are in place for it to be recorded as legitimate research, and risks of potential harms are identified and managed, including via ethical review by UREC, and any material collected stored securely.

The aim of the policy is to prevent researchers from undergoing investigation from external authorities for perceived illegal activity.

The policy allows the University to protect academic freedom, and the reputation of the University as a centre for properly conducted research and KE activity, whilst balancing the need to protect colleagues and students, and comply with relevant legislation.

There remains a risk that this policy may not wholly protect researchers from action by another countries' security or legal authorities in particular, but also the UK authorities. The Principal Investigator (PI) needs to identify, familiarise and mitigate any risks on an ongoing basis and should be aware that the nature of such research can raise suspicions from others. All PIs should undergo the University's Prevent training module.

The Home Office's Statutory *Prevent duty guidance: for higher education institutions in England and Wales* states universities are responsible for the oversight of 'security sensitive research' in order to enable the university to identify legitimate research and KE activity from non-research and KE purposes. The Home Office advises universities to employ the *Universities UK guidance* for managing and having oversight of such research, whilst enabling legitimate researchers to be protected.

The *Universities UK guidance* states:

"*There is a range of legislative provisions that relate to the storage and circulation of security-sensitive material. Section 58 of the Terrorism Act 2000 makes it an offence if a person 'collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism'. A modification by the Counter-Terrorism and Border Security Act 2019 also introduced the offence of viewing or otherwise accessing via the internet documents or records containing information which is likely to be useful to a person committing or preparing an act of terrorism. There is a defence if the information is used for academic research purposes."*[2]

The *Guidance* 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 defence under the Terrorism Act 2006".*[3]

Universities UK acknowledges that not all security-sensitive research relates to terrorism, and other areas could include research and KE activity commissioned by the Ministry of Defence, research and KE activity into extremism of animal rights campaigners, or IT encryption design for public bodies or businesses, amongst examples mentioned in the Guidance.

3. DEFINITION

There is currently no legal definition of 'security sensitive'. It is therefore not possible to provide an exhaustive list of potential security sensitive areas; however, it is likely to include (but not be limited to), research and KE activity into:

- Extremism, terrorism or radicalisation;
  - I. Extremism is defined in the Home Office's Statutory Prevent duty guidance for England and Wales under the Counter Terrorism and Security Act 2015 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'4
  - II. Radicalisation i.e. a process by which a person may come to support terrorism or extremist ideologies often associated with terrorist or extremist groups of political, social or religious nature.
- Organisations that could breach counter-terrorism legislation under the Terrorism Act (2006), for instance extremist animal rights or Far Right groups.
- Prohibited organisations.
- Cyber-terrorism and/or cyber-security
- Criminal or illegal activity
- Any area(s) which require the acquisition of security clearances.
- Any area(s) commissioned by the military or under an EU security call.

4. PROCESS

A Standard Operating Procedure (SOP) is being developed by UREC for researchers and RECs to follow. In the meantime, below is a summary of the process at the current time:

The Principle Investigator (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. In the case of taught student research projects, the Supervisor is viewed as the PI and must guide the student in completing their Research and KE Ethics Form via the VRE. Doctoral Students should liaise closely with their Supervisory team.

The PI must commence a VRE Research and KE Ethics Application form, which will further assist in ascertaining and recognising the types of potential harms of any research and KE activity, including security sensitive. The form contains questions on security sensitive research and KE, and further guidance in completing these questions is available in the *'Security Sensitive Ethics Application Guidance Note for Researchers'* and will in due course be available in the VRE question 'information' fields, as built in guidance itself.

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.

In the case of security sensitive research and KE activity a completed risk assessment should be provided alongside the Research & KE Ethics Application Form via the VRE.

If the PI submits a Form but does not identify any security sensitive issues, the receiving CREC must promptly and without delay progress the Form via the VRE, only to UREC, for UREC to undertake an ethics review and request the research is correctly identified as security sensitive, if appropriate.

All research and KE activity designated as security sensitive will require a secure store for any security sensitive materials to be collected, which is only accessible to the PI, to hold information or data related to the research or KE activity, this information or data must not be transmitted by the PI.

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. Your IP address is traceable, and authorities will be able to reach you through this, they may contact the University to confirm whether the material or information you access, view, download, store or transmit is part of legitimate research and KE activity which is recorded at the University, and whether it has undergone ethics review.

Remember, 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 means. **Contravention of this would be deemed illegal**.

All work must continue to be carried out within the University's Information Systems Acceptable Use Policy.

4.1 SECURE STORE

Once your Research and KE Ethics Application has undergone review and you have been provided Approval with Conditions you will be guided by the RKEO in conjunction with Information Systems and Services Team (ISS Team) to the software required. You must not commence any security sensitive material collection until the secure store has been set-up for you, with restricted access to only yourself.
Researchers may have access to hard copy material, which following IT advice, the storage or use of would be discussed and agreed on a case by case basis (during or shortly after an ethical review).

For collaborative projects where data is being stored at a third-party external organisation, written confirmation as to their storage arrangements must be obtained. These should be included as part of the security-sensitive risk assessment.

Should the University be approached by the authorities, or for its own research governance audit requirements, the University store will be accessed by the University's Prevent Lead, or Chair of UREC in the Prevent Lead's absence.

This will be to confirm to authorities that your research and KE activity is legitimate and has undergone ethics review and approval (by UREC), and a record of this kept on the VRE which will act as the University's confidential internal 'register'.

5. SECURITY SENSITIVE ETHICS APPLICATION GUIDANCE NOTE FOR RESEARCHERS

A guidance note with advice and web-links to help with specific questions within the Research and KE Ethics Application Form can be obtained from 'research governance webpage link'. In due course this guidance will be built into the VRE Ethics Application Form.

6. SAFEGUARDING

The University has a duty of care to its staff and students, and in order to help identify, prevent and mitigate any potential harms, the PI must undertake to complete a risk assessment which will be dynamic i.e. revisited as appropriate. It is advised that as well as obvious data leakage risks, the risk assessment includes consideration to any potential psychological impacts of the research and KE activity for the researcher(s).

7. STIGMATISATION

In line with Universities UK *Guidance* and the University's own equality, diversity and inclusion principles, the existence of a research ethics review process to manage such research and KE activity, and the availability of safe storage for security-sensitive material will not stigmatise any specific groups.

REFERENCES:

1, 2 and 3: Universities UK's (UUK's) *Oversight of Security Sensitive Research Material at UK universities*, 2019.

4: Home Office, Statutory Guidance: *Prevent duty guidance* for England and Wales , 2021.

CONTACT:

For enquiries about this policy please contact Research-knowledge-exchange-office@westminster.ac.uk, for enquiries concerning a specific research proposal please contact the UREC at research-ethics@westminster.ac.uk