Richmond, the American International University in London
November 2021
Version 1

# Security Sensitive Research Policy

## Introduction

1. The UK Counter-Terrorism and Security Act 2015 imposes a duty on Universities to "have due regard to the need to prevent people from being drawn into terrorism". Similarly, the Prevent Duty guidance for Higher Education England and Wales places responsibilities on universities on the oversight of security-sensitive research.

2. This requires the University to have policies and processes in place for staff or students working on sensitive, radical, or extremism-related research, which has been defined as research involving groups that are on the Home Office list of 'Proscribed terrorist groups or organisations'.

3. Research material which could be classified as "security-sensitive" may include anything which could be interpreted as promoting, endorsing, or planning terrorism, radicalisation, or extremism. It can be a criminal offence to possess any article in circumstances which give rise to a reasonable suspicion that the possession is for a purpose connected with the commission, preparation, or instigation of an act of terrorism, even where the article is already publicly accessible elsewhere.

## Purpose

4. The security-sensitive research policy aims to balance academic freedom to pursue academic research with the need to protect staff, students, and compliance with relevant legislation.

5. Adherence to the policy will allow the University to ensure the welfare of staff and students who undertake security-sensitive research by recognising the potentially radicalising and/or distressing effects of viewing security-sensitive material.

6. The policy aims to ensure compliance with the Counter-Terrorism and Security Act 2015 by ensuring that research activities are conducted in such a way that individuals *are not drawn into terrorism*.

7. The policy enables the University to assist external authorities by demonstrating that the actions of staff and students who are involved in security-sensitive research are part of legitimate research activities. However, the University cannot guarantee protection from investigation or prosecution by external authorities.

8. The policy does not replace the requirement for other approvals that research projects may require, for example, those where ethical considerations apply and/or where there are specific safety considerations. The policy also excludes considerations of confidentiality or non-disclosure that may be required under law.

## University Ethical Review Process

9. Research into security-sensitive, radical, or extreme material must include a risk assessment that has been reviewed and approval granted by the University before the research can commence.

10. Students must discuss potentially security-sensitive research at the earliest point with their supervisor of the research project.

11. Research that is identified as within the security-sensitive policy remit must undergo the research ethics approval process before the research commences.

12. Any research that is identified as within the security-sensitive policy, students are required to complete the Security-Sensitive Research Safety Questionnaire together with the Student Application Form for Research Ethics Approval. Student must indicate the main risks of the research in the application form and how these will be mitigated.

13. The security-sensitive research safety questionnaire and student application form for research ethics approval will be initially reviewed by the University's Research Ethics Committee for completeness and to identify all potentially security-sensitive issues.

14. On completion of the approval process, the Research Ethics Committee will issue a confirmatory email to the student and the supervisor of the research project informing them the research can now commence.

15. If the approval process identifies significant risks or infrastructure limitations, the Research Ethics Committee will issue their decision in a refusal email to the student and the supervisor of the research project explaining on what grounds this decision has been taken.

16. The student may appeal this decision in writing to the Provost within one month of receipt of the refusal email. The basis of the appeal must be based on (one or more of) the grounds of:
    a. procedural irregularity or;
    b. a decision was manifestly unreasonable or influenced by prejudice or bias, or perception thereof, on the part of the decision-maker(s)

17. Any change in scope, documents, or research design of the security-sensitive research must undergo a subsequent research approval review. An updated track changed version of the registration form and risk assessment must be submitted to the Research Ethics Committee.

18. Details of all security-sensitive research projects, including whether they have been granted approval or not will be recorded on a University-wide security-sensitive research register to be maintained by the Research Ethics Committee.

## Accessing, Safe Storage, and Disposal of Security-Sensitive Material

19. When accessing security-sensitive material, students are recommended to use the University network (including the wireless network and VPN) and computers which are

University-owned. This will help to demonstrate that these activities are a legitimate part of their research.

20. Students who access potentially security-sensitive research material should not share or disseminate such material, even where material is already publicly accessible elsewhere, and should ensure that appropriate systems are in place for the storage and handling of such material.

21. All security-sensitive material must be stored and transmitted only for the approved research purposes. It should only be accessible to the approved student, their supervisor and any appropriate authorities who are legally entitled to access that material. No data should be stored on local computers or external storage devices.

22. Security-sensitive material must be disposed of in an appropriate manner. Security-sensitive material must only be stored for as long as required to conduct the research and comply with any legal requirement or best practice guidance concerning maintaining original data.

## Handling External Enquiries

23. Enquiries from Police or external security services must be directed in the first instance to the Head of Security. The IT department and department of Registry, Admissions and Quality Assurance (RAQA) will co-ordinate with the Head of Security in considering and granting requests and for ensuring access is chaperoned.

## Discovering Security-sensitive Materials

24. All staff or students who become aware of the problematic use of sensitive-security related content (outside of their usual class or research activities) by peers or colleagues, or if sensitive materials are discovered on campus related to terrorism or extremism, have a duty to contact the Security Department in the first instance.

## VERSION MANAGEMENT

| **Responsible Department:** | | | |
|---|---|---|---|
| **Approving body: Academic Board** | | | |
| **Version no.** | **Key Changes** | **Date of approval** | **Date of effect** |
| 001 | New policy | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | **Restricted access?** *Tick as appropriate* ☐ **Yes** ☒ **No** | |