**Security Sensitive Research Policy**

1. **Introduction**
2. Amity University [IN] London seeks to ensure that the freedom to pursue academic research is upheld and balanced with the need to protect both staff and students, and to ensure compliance with relevant legislation
3. This Policy does not replace the requirement for other approvals that projects may require e.g. those where ethical considerations apply and/or where there are specific safety considerations. This Policy also excludes considerations of confidentiality or non-disclosure that may be required under law or as part of contractual arrangements with funders.
4. The Prevent Duty guidance for Higher Education England and Wales places responsibilities on Universities on the oversight of “security-sensitive research”; *To enable the university to identify and address issues where online materials are accessed for non-research purposes, we would expect to see clear policies and procedures for students and staff working on sensitive or extremism-related research”(*<https://www.gov.uk/government/publications/prevent-duty-guidance>
5. **Purpose**
6. The security-sensitive research policy aims to ensure that those working with security-sensitive research material are suitably protected and are not in infringement of the law. In operating this Policy, the University seeks to ensure that the freedom to pursue academic research is upheld, balanced with the need to protect both staff and students, and to ensure compliance with relevant legislation.
7. Specifically, but not exclusively, 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. Adherence to this policy will allow the University to assist external authorities by demonstrating that the actions of the researcher(s) were part of legitimate research activities and fulfil its ‘Prevent Duty’ in a proportionate and risk-based approach
8. **Scope**
9. This Policy covers security-sensitive research as defined in the Definitions section (5). This Policy covers research activities and related activities i.e. fundraising, providing consultancy, innovation, commercial and analytical services and the setting up and running of University spin-out companies (if any). It excludes teaching. This Policy applies to the following groups of people as they are undertaking the activities associated with the activities described above.
10. All University staff including agency staff, (1) Visiting Staff and Visiting Professors, (2) staff visiting from other institutions undertaking or supervising research at or for the University; and (3) Undergraduate and postgraduate students (both taught and research), Undergraduate and master’s level research would not normally involve accessing materials described above but where this is required by the department, the policy will apply. The Policy covers activities undertaken, by the above, in the UK or in any overseas location.
11. The Policy also covers research that may be led by another Institution or where a Amity University [IN] London researcher is contributing to research. It should be noted that researchers based overseas or researchers travelling to overseas locations will need to abide by local laws and regulations, for example in regard to collecting and holding sensitive data.
12. Note that compliance with the policy does not guarantee protection from investigation or prosecution by external authorities. This process may not protect individuals from action taken by other countries’ security or legal agencies.
13. **Equality Analysis**
14. This policy has been reviewed for equality impact and it is not anticipated that this policy will have any negative effect on any protected groups under the Equality Act 2010.
15. **Definitions**
16. ***Security-Sensitive Research*** for the purpose of this policy relates to research involving one or more of the categorizes below;
17. Research that involves the acquisition of security clearances, for example research or materials that are covered by the Official Secrets Act 1989 and the Terrorism Act 2006 (http://www.legislation.gov.uk/ukpga/1989/6/contents and http://www.legislation.gov.uk/ukpga/2006/11/contents)
18. Research into extremism or radicalization and/or which involves materials that could be considered ‘extremist’ or which could be used for the purpose of radicalization
19. Research or materials used for research projects commissioned by the military or under an EU security call
20. ***Extremism*** is defined in the (Prevent) Statutory Guidance to HEIs under Section 29 of 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'. It also includes calls for the death of members of UK armed forces, whether in this country or overseas.
21. Extremist material is information in whatever form that supports such views.
22. ***Radicalization*** is defined as the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
23. Radical Material is information in whatever form that can result in radicalization
24. **Legislative context**

Counter-Terrorism and Security Act 2015; Official Secrets Act 1989; Terrorism Act 2006 Data Protection Act 1998; Health and Safety at Work Act 1974; Export Control Act 2002; Equality Act 2010

1. **Policy Principles**
2. *Ensuring researcher wellbeing* alongside the Universities Health and Safety Policy and Ethics Policy, this Policy is designed to ensure that those involved in security-sensitive research can conduct that work safely.
3. *Understanding the University’s involvement in security-sensitive research* All security-sensitive research must be identified so that it can be subject to Confirmation and Registration before the research begins and to aid authorities with external enquiries.
4. *A risk-based approach to security-sensitive research* This Policy is not designed to stop research or restrict academic freedom but rather to ensure that any risks are appropriately managed. It is not possible to define fully in advance all the types of security-sensitive research that could be undertaken and hence the University expects that a detailed and specific risk assessment be produced for any and all such work. Research into security-sensitive, radical or extreme material must include a risk assessment that has been reviewed and confirmation granted by the University before the research can commence.
5. *Safe storage and transmission of security-sensitive material* All security-sensitive materials must be stored and transmitted in a way that means it is available only for the approved research and to the approved researchers and to any appropriate authorities who are legally entitled to access that material.
6. *Safe disposal 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.
7. **Procedures**

The Identification and Confirmation procedures are described in the work flow diagram included as Annex: 1.

1. *Identification*: The Lead Researcher (usually Supervisor or Principal Investigator; i.e. University employee) is responsible for assessing whether the research is covered by this Policy. If the Research is not being led by Amity University [IN] London an alternative” Amity Principal Investigator” at Amity University [IN] London must be identified.
2. Researchers are encouraged to discuss potentially security-sensitive research at the earliest point, students with their Supervisor, or members of staff with their Head of Unit/. Any special provisions, facilities or resources such as access to security sensitive web sites that may contravene the acceptable use policies or secure storage of materials, must be identified as early as possible and agreed with the relevant department, including but not limited to IT Services and Estates and Facilities. Where there are likely to be cost implications to conducting the research, discussion must be had before submission of the grant or contract award
3. *Registration*
4. Research that is identified as within the security-sensitive policy remit must be registered and undergo the confirmation process before the research commences. A security-sensitive research registration form must be completed. A security-sensitive research risk assessment must also be completed indicating the main risks and how these will be mitigated. Proper consideration should be given in completing the risk assessment to the University’s policies and procedures that may be relevant, including but not limited to IT, procurement, health and safety, insurance and travel. Only the security-sensitive research registration form and risk assessment must be sent to the Research Unit (RU) at the email address indicated on the forms.
5. In the event that the security-sensitive research also involves any of the criteria triggering an ethical review, then the assessment of the security- sensitive research and mitigations will take place as part of the ethics review process.
6. *Confirmation Process*
7. The security-sensitive research registration form and risk assessment will be initially reviewed by RU for completeness and to identify all potentially security sensitive issues that require expert review.
8. RU will co-ordinate expert reviews of the risk assessment liaising with appropriate personnel and policy holders from across the University. RU will feedback to the Lead Researcher if the expert reviewers require additional information or changes to procedures or risk mitigation before confirmation to commence can be granted. On completion of the Confirmation process, RU will issue a confirmatory email to the Lead Researcher informing them the research can now commence.
9. In the event that the confirmation process identifies significant reputational risks or infrastructure limitations, the decision to grant confirmation will be referred to the Head of Research will inform RU by email and issue their decision in a refusal email to the Lead Researcher explaining on what grounds this decision has been taken.
10. The Lead Researcher may appeal this decision in writing to the Principal within one month of receipt of the refusal email. The basis of the appeal must be on (one or more of) the grounds of (1) procedural irregularity or (2) equality.
11. Any change in scope, documents, or research design of the security-sensitive research must undergo a subsequent confirmation review. An updated track changed version of the registration form and risk assessment must be submitted to RU and where an ethical review was also applicable it will be considered
12. *Security-Sensitive Research Register*
13. Details of all security-sensitive research projects, including whether they have been granted Confirmation or not will be recorded on a University-wide security-sensitive research register to be maintained by the Research Unit (RU) Security-sensitive registration forms and risk assessments will be held on the University secure network. An updated copy of the University-wide security sensitive research register will be issued to the Head of Security after every complete Confirmation process.
14. *Handling Security-sensitive materials/data*
15. Researchers must only use agreed IT facilities and equipment approved by the university to carry out their research. It is not permissible to use personal devices to save, transport and/or transmit any of the data, only University approved, and encrypted devices are permitted. This will ensure activities can be identified as a legitimate part of their research. Any data, files or electronic items used or produced during projects that fall under this Policy must be stored appropriately in accordance with the completed data management plan and risk assessment. No data should be stored on local computers or external storage devices.
16. For collaborative projects where data is being stored at a third party organization, written confirmation as to their storage arrangements must be obtained. Where the sharing of raw data beyond the University research team is unavoidable the mechanisms for sharing and risk mitigations must be addressed in the risk assessment. Paper or other physical materials and media relating to security-sensitive research must, wherever practicable, be scanned and/or uploaded to the allocated secure server folder and hard copies should subsequently be securely destroyed.
17. *Handling External Enquiries*
18. Enquiries from Police or external security services must be directed in the first of instance to the Head of Security. The ICT Unit and the Research Unit will co-ordinate in considering and granting requests and for ensuring access is chaperoned.
19. *Security-sensitive materials*
20. All staff or students who become aware of colleagues who may be engaging in sensitive security related activities, or if sensitive materials are discovered on campus related to terrorism or extremism, have a duty to contact their Head of Unit in the first instance. Th Head of Unit will check if the research is registered on the Security-Sensitive Research Register and take appropriate action.

1. *Breach of the Policy*
2. Intentional breaches of this policy will be considered as research misconduct and investigated through the “Code of Practice on Handling Allegations of Research Misconduct”
3. **Governance Requirements**
4. Responsibilities
5. *Postgraduate Researchers* are:
* Adhering to the procedures for undertaking sensitive research as agreed through the confirmation process. Including but not limited to, ensuring proper storage of data and research materials, dissemination (if any) and secure destruction of research materials or outcomes.
* Raising any risks relating to the provisions of this Policy that may emerge during the research programme. This would include risks to the well-being of colleagues.
1. *Lead Researcher (typically Supervisors, Principal Investigators)*
2. It is the lead researcher’s responsibility to ensure that all security-sensitive research has been registered and that research does not start before confirmation to commence has been received. They are also responsible for reregistering if there are material or research design changes.
3. The Lead Researcher is also responsible for ensuring the necessary physical or IT provisions are in place before security-sensitive research is undertaken.
4. The Principal Investigator Reviews the progress of the research and ensure risk assessments and risk mitigations are updated as necessary
5. *Heads of Unit/Department*

1. Heads of Unit/Department have a responsibility to ensure staff are aware of this Policy and to challenge staff who are conducting security-sensitive research to ensure they have complied with this Policy, in particular obtaining Confirmation to commence for that research.
2. *Research Integrity and Research Unit*
3. The Research Unit has the following responsibilities
* To act as a point of contact for those who may wish to undertake security sensitive research as defined in this Policy.
* To co-ordinate the review of all security-sensitive research project registrations and risk assessments, liaising with personnel and policy holders from across Amity University [IN]London, and seek legal advice where necessary.
* To manage and co-ordinate the implementation of this Policy and to ensure it is kept updated. In particular, to maintain a register of all security-sensitive research being undertaken and providing this to the Head of Research Unit
1. *Head of Research*
2. The Head of Research Unit has the following responsibilities:
* To ensure this policy is incorporated into any Prevent related communications or initiatives.
* To ensure the content of this Policy is included within relevant training courses offered to researchers and other staff
1. **Implementation**
2. *Broad University level training is provided to:*
* to all staff (via Moodle): Prevent Duty workshop In-depth training for those carrying out expert reviews or likely to advise staff and students on requirements under the Policy; (a) Including members of the University
* to researchers working in this area of research to include. The training programme include: (1). Their specific duties under this Policy (2). Handling security-sensitive materials (3). Handling and escalating concerns or enquiries about security-sensitive research The University’s ethics guidance webpages to be updated and added to with security-sensitive specific details. All forms and guidance relating to this policy will be made freely available online.

**Annex 1. Security‐Sensitive Research Checklist**

|  |  |
| --- | --- |
| **Security-Sensitive Research Criteria** | **Add a “X” to all that apply**  |
| 1. Does the work involve research or materials that are covered by the Official Secrets Act 1989 and the Terrorism Act 2006?
 | **☐** |
| 1. Does the work involve research into extremism or radicalization and/or involve materials that could be considered ‘extremist’ or which could be used for the purpose of radicalization?
 | **☐** |
| 1. Has the research been commissioned by the military or security services?
 | **☐** |
| 1. Has the research been commissioned under an EU Security Call?
 | **☐** |
| 1. Does the work require security clearances to undertake the research?
 | **☐** |
| 1. Are there any other aspects not covered by the criteria above that could make the research security-sensitive?
 | **☐** |

If you tick any of the above, the proposed research is highly likely to fall within the security-sensitive research policy and you are required to follow the Security-sensitive research registration and confirmation process. If you are unsure, then you are advised to seek general advice from RU (Research Unit)

Please note specific details of the security sensitive research, and attachments should not be sent to RU, if you feel this is necessary, please defer your enquiry to the Head of Research .

**Definitions:**

**Extremism** is defined in the (Prevent) Statutory Guidance to HEIs under Section 29 of 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'.* It also includes calls for the death of members of UK armed forces, whether in this country or overseas.

Extremist material is information in whatever form that supports such views.

**Radicalisation** is defined as the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Radical Material is information in whatever form that can result in radicalization

**Annex 2**

**Security‐Sensitive Research Registration Form**

|  |  |
| --- | --- |
| **Section A –Security-sensitive research Criteria** **Please confirm the criteria that has triggered this registration form.**  | **Add an “X” to all** **that apply** |
| 1. Does the work involve research or materials that are covered by the Official Secrets Act 1989 and the Terrorism Act 2006?
 | **☐** |
| 1. Does the work involve research into extremism or radicalisation and/or involve materials that could be considered ‘extremist’ or which could be used for the purpose of radicalisation?
 | **☐** |
| 1. Has the research been commissioned by the military or security services?
 | **☐** |
| 1. Has the research been commissioned under an EU Security Call?
 | **☐** |
| 1. Does the work require security clearances to undertake the research?
 | **☐** |
| 1. Are there any other aspects not covered by the criteria above that could make the research security-sensitive?
 | **☐** |

|  |  |
| --- | --- |
| **Section B – Basic Project Details Please complete this next section as fully as possible. If you are completing an ethics application also, Section B can be left blank and reference made to a completed Ethics Application Form.**  | **Guidance** |
| 1. Title of project
 |  |
| 1. Project Code:
 |  |
| 1. Start and End dates for the Project
 |  |
| 1. Name of person submitting form
 | Main contact for any correspondence |
| 1. Is this project a collaboration with an external body? Please also explicitly indicate which organisation is leading the research
 | If yes, please state the collaborators in the space provided e.g. another Higher Education Institution (HEI), company |
| 1. Is the research covered by a UK or other government security classification? If so, please give details.
 |  |
| 1. Where will the research be carried out? Please be sure to include details of any work carried at an overseas location?
 |  |
| 1. Are you applying for any other approvals for this research? If so please indicate what they are.
 | Include University Ethics /Research Committee, Head of Research |

|  |
| --- |
| **Section C – Declarations** Please read each declaration and confirm your agreement by adding a signature below. Electronic signatures are acceptable. If you do not have an electronic signature, please print the form, sign and then send a scanned PDF copy of the form alongside the unsigned word document to RU |
| 1. I confirm that I have discussed the research project with my Head of Department/Unit
 |
| 1. I confirm that I have completed the online Prevent Duty training workshop.
 |
| 1. I confirm that the research will not commence until confirmation to do so is received
 |
| 1. I confirm that I have completed and will abide by the security-sensitive risk assessment
 |
| 1. I understand and accept that RU will be registering this project on the Universities’ security-sensitive research register and will provide this register to external agencies where necessary
 |
| 1. I confirm I have completed a Data Management Plan
 |
| 1. I understand that compliance with this policy does not guarantee protection from investigation by authorities in the UK and elsewhere
 |
| 1. I confirm that I will abide by the University’s Security-sensitive research Policy and all related policies
 |
| Signature……………………………………………………………….Name…………………………………………………………………….Department/Unit………………………………………………………….Date form signed…………………………………………………………. |  |

s