Security-sensitive Research Policy

Operational Owner:	Sophie Wehrens
Executive Owner:	David Sampson
Effective date:	16 December 2018
Review date:	December 2020
Related documents:	Information Security Policy Email Policy IT Acceptable Use Policy and Guidance Notes Using Your Own Device Policy Ethics Policy Ethics Handbook for Teaching and Research Code of Practice on Handling Allegations of Research Misconduct Code on Good Research Practice Health and Safety Policy Children and Adults At Risk (Safeguarding) Policy Dignity at Work and Study Policy Security-sensitive research Workflow Diagram (Appendix 1) Security-sensitive research checklist (Appendix 2) Security-sensitive research registration form (Appendix 2) Security-sensitive research risk assessment (Appendix 2) Guide for Researchers on Conducting security-sensitive research (Appendix 3)

Approval History

Version	Reviewed by	Approved by	Date
1	Gill Fairbairn - First Draft		15 Sept 2016

	Research Integrity and Governance Committee		15 Sep 2016
	Equality and Diversity: Jo McCarthy-Holland Reviewed for equality impact – no negative impact identified, subject to ongoing review.		16 Nov 2016
	Executive Board		17 Nov 2016
2	Ali Alshukry - Minor updates, clarifications on scope under the policy, addition of webpages blocking		14 June 2018
	Research Integrity and Governance Committee		14 Jun 2018
	Senate		30 Oct 2018

1 Introduction

Universities play a vital role in carrying out research on issues where security-sensitive, radical or extreme material is relevant. It is not the intention of this policy to prevent or restrict such research but is rather to ensure processes are in place and risks are understood and managed.

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. However, the University cannot guarantee protection from investigation or prosecution by external authorities.

With this Policy, the University 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.

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.

The Prevent Duty guidance for Higher Education England and Wales https://www.gov.uk/government/publications/prevent-duty-guidance 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"

1.1 Purpose

1.1.1 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.

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.

1.2 Scope

1.2.1 This Policy covers security-sensitive research as defined in the Definitions section (1.3).

This Policy covers research activities and related activities i.e. providing consultancy, innovation, and commercial and analytical. It excludes teaching.

This Policy applies to the following groups of people as they are undertaking the activities associated with the activities described above.

- all University staff including agency staff, Honorary Staff and Emeritus Professors
- staff visiting from other institutions undertaking or supervising research at or for the University; and
- Undergraduate and postgraduate students (both taught and research), whether

registered here or on temporary placement. Undergraduate and Master's level research would not normally involve accessing security-sensitive 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. The Policy also covers research that may be led by another Institution or where a University of Surrey 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.

Note: Compliance with the policy does not guarantee protection from investigation or prosecution by external authorities. In particular, this process may not protect individuals from action taken by other countries' security or legal agencies.

1.3 Definitions

1.3.1 **Security-sensitive Research,** for the purpose of this policy, relates to research involving one or more of the categorises below;

i) 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**)

ii) Research into extremism or radicalisation and/or which involves materials that could be considered 'extremist' or which could be used for the purpose of radicalisation

iii) Research or materials used for research projects commissioned by the military or under an EU security call and requires security clearances to undertake the research

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 radicalisation.

2 Policy Principles

2.1 Principles

2.1.1 Ensuring Researcher Well Being

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.

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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.

2.2 Procedures

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

2.2.1 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 the University of Surrey an alternative ”Surrey Principal Investigator” at the University of Surrey must be identified.

The security-sensitive research checklist (Appendix 2) is available to University of Surrey staff if they are unsure if their research falls within the Policy.

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 Department.

Any special provisions, facilities or resources such as access to security sensitive websites that may contravene the acceptable use policies, be inaccessible due to the universities web filtering processes 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.

2.2.2 Registration

Research that is identified as within the security-sensitive policy remit must be registered and undergo the confirmation process (2.2.3) before the research commences.

A security-sensitive research registration (Appendix 2) form must be completed.

A security-sensitive research risk assessment (Appendix 2) 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, Secretariat and Legal, and travel. Only the security-sensitive research registration form and risk assessment must be sent to the Research Integrity and Governance Office (RIGO) at the email address indicated on the forms.

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. The University of Surrey ethics review process is described in the "Ethics Handbook for Teaching and Research".

2.2.3 Confirmation Process

The security-sensitive research registration form and risk assessment will be initially reviewed by RIGO for completeness and to identify all potentially security-sensitive issues that require expert review.

RIGO will co-ordinate expert reviews of the risk assessment liaising with appropriate personnel and policy holders from across the University of Surrey. RIGO will feed back 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, RIGO will issue a confirmatory email to the Lead Researcher informing them the research can now commence.

RIGO will liaise with IT to notify them of a confirmed security-sensitive research project requiring access to blocked websites. This access will be time limited and monitored and must be detailed in the risk assessment. Monitoring reports may be requested from IT by the Head of Department or Supervisor for academic staff and research students respectively.

In the event that the confirmation process identifies significant reputational risks or infrastructure limitations, the decision to grant confirmation will be referred to the Vice-Provost (Research and Innovation) (VPRI). The VPRI will inform RIGO by email and issue their decision in a refusal email to the Lead Researcher explaining on what grounds this decision has been taken.

The Lead Researcher 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 on (one or more of) the grounds of (i) procedural irregularity or (ii) equality.

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 RIGO and where an ethical review was also applicable it will be considered as an amendment in accordance with the "Ethics Handbook for Teaching and Research"

2.2.4Security-Sensitive Research Register

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 Integrity and Governance Office (RIGO) .

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 or at least every 6 months.

2.2.5Handling Security-sensitive materials/data

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 of Surrey 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.

For collaborative projects where data is being stored at a third party organisation, written confirmation as to their storage arrangements must be obtained.

Where the sharing of raw data beyond the University of Surrey 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.

2.2.6Handling External Enquiries

Enquiries from Police or external security services must be directed in the first instance to the Head of Security. The IT department and RIGO will co-ordinate with the Head of Security in considering and granting requests and for ensuring access is chaperoned.

2.2.7Discovering Security-sensitive materials

All staff or students who become aware of colleagues who may be engaging in security sensitive related activities, 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.

Security will check if the research is registered on the Security-Sensitive Research Register and take appropriate action.

2.2.8Breach of the Policy

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

3.1 Responsibility

Researchers (i.e. those involved in undertaking research including Postgraduate Researchers)

- 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.

Lead Researcher (typically Supervisors, Principal Investigators)

- 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 re-registering if there are material or research design changes.

- The Lead Researcher is also responsible for ensuring the necessary physical or IT provisions are in place before security-sensitive research is undertaken.
- Reviewing progress of the research and ensuring risk assessments and risk mitigations are updated as necessary

Heads of Department/School

- Heads of Department/School 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.

Research Integrity and Governance Office

- 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 the University of Surrey, 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 Security.

VPRI and University Prevent Group

- 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.

3.2 Implementation / Communication Plan

3.2.1 Training

Broad University level training:

• Provided to all staff via the SurreyLearn compulsory modules: Prevent Duty module

A training programme will be made available for researchers working in this area of research to cover:

1. Their specific duties under this Policy
2. Handling security-sensitive materials
3. Handling and escalating concerns or enquiries about security-sensitive research

3.2.2 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.

3.3 Exceptions to this Policy

3.3.1 Any activities outside Section 1.2.1.

3.4 Review and Change Requests

3.4.1 This Policy should be reviewed every 2 years, unless changes in regulations, other policies or improvements to its implementation require an interim update. Minor interim changes such as change of a role title or other titles or names or typos, which do not change the meaning of the Policy will be handled by the operational owner. Major changes, i.e. anything that alters the meaning of the Policy or are substantial, will be submitted via the full approval route.

3.5 Legislative context

3.5.1 Legislation

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

3.5.2 Other guidance

Universities UK guidance, available at;
http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/oversight-of-security-sensitive-research-material-in-uk-universities.aspx
(https://www.gov.uk/government/publications/prevent-duty-guidance)

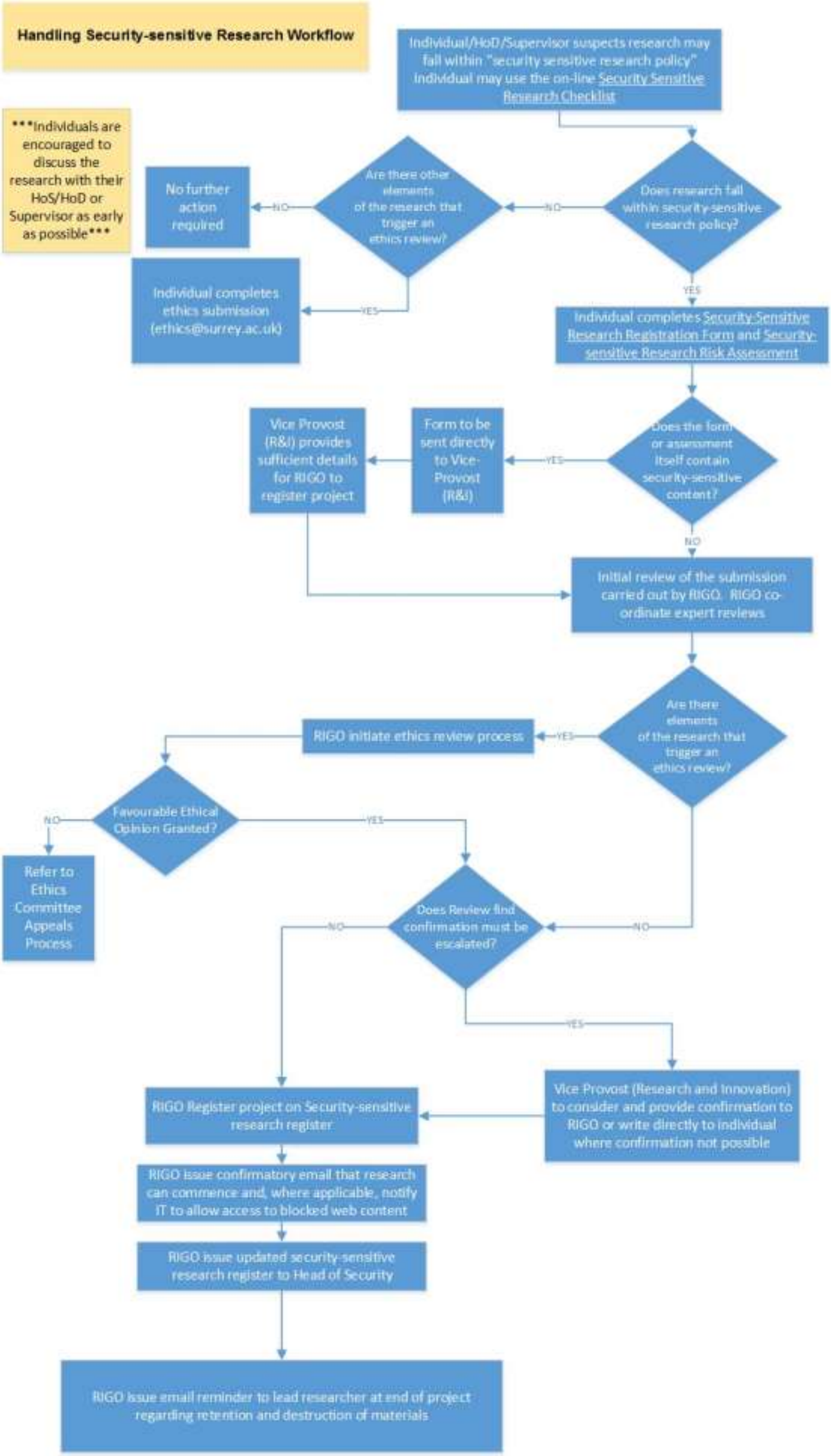
'Prevent Duty Guidance for higher education institutions in England and Wales', dated July 2015, available at;
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

3.6 Stakeholder Statements

3.6.1 Equality: 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.

3.6.2 Health & Safety: This policy supports the principles articulated in the Health and Safety Policy which apply to this context as well.

Appendix 1 - Security-sensitive Research workflow


Handling Security-sensitive Research Workflow
Individuals are encouraged to discuss the research with their HoS/HoD or Supervisor as early as possible
Individual/HoD/Supervisor suspects research may fall within "security sensitive research policy" Individual may use the on-line Security Sensitive Research Checklist
Does research fall within security-sensitive research policy?
NO
Are there other elements of the research that trigger an ethics review?
NO
No further action required
YES
Individual completes ethics submission (ethics@surrey.ac.uk)
YES
Individual completes Security-Sensitive Research Registration Form and Security-sensitive Research Risk Assessment
Does the form or assessment itself contain security-sensitive content?
YES
Form to be sent directly to Vice-Provost (R&I)
Vice Provost (R&I) provides sufficient details for RIGO to register project
NO
Initial review of the submission carried out by RIGO. RIGO co-ordinate expert reviews
Are there elements of the research that trigger an ethics review?
YES
RIGO initiate ethics review process
Favourable Ethical Opinion Granted?
NO
Refer to Ethics Committee Appeals Process
YES
NO
Does Review find confirmation must be escalated?
NO
YES
Vice Provost (Research and Innovation) to consider and provide confirmation to RIGO or write directly to individual where confirmation not possible
RIGO Register project on Security-sensitive research register
RIGO issue confirmatory email that research can commence and, where applicable, notify IT to allow access to blocked web content
RIGO issue updated security-sensitive research register to Head of Security
RIGO issue email reminder to lead researcher at end of project regarding retention and destruction of materials

Appendix 2 - Security-Sensitive Research Checklist

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, the Terrorism Act 2006 and/or covered by the counter terrorism Act 2015??	□
2. 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?	□
3. Has the research been commissioned by the UK military or security services and requires security clearances to undertake the research?	□
4. Has the research been commissioned under an EU Security Call and requires security clearances to undertake the research?	□
5. Has the research been commissioned by non-UK military or security services?	□
6. 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 RIGO (Research Integrity and Governance Office)

Please note specific details of the security sensitive research, and attachments should not be sent to RIGO, if you feel this is necessary, please defer your enquiry to the Vice-Provost (Research and Innovation)

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 radicalisation.

Security-Sensitive Research Registration Form

This form can be completed electronically, electronic signatures are acceptable for Section C: Declarations.

Once completed please sent the form to RIGO (rigo@surrey.ac.uk), along with a completed Risk Assessment.

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, the Terrorism Act 2006 and/or covered by the counter terrorism Act 2015?	☐
2. 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?	☐
3. Has the research been commissioned by the UK military or security services and requires security clearances to undertake the research?	☐
4. Has the research been commissioned under an EU Security Call and requires security clearances to undertake the research?	☐
5. Has the research been commissioned by non-UK military or security services?	☐
6. 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
.	Title of project	
2.	UNCLE ref: and/or Finance Project Code:	
3.	Start and End dates for the Project	
4.	Name of person submitting form	Main contact for any correspondence
5.	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
6.	Is the research covered by a UK or other government security classification? If so please give details.	

7.	Where will the research be carried out? Please be sure to include details of any work carried at an overseas location?	e.g. In the UK at University of Surrey, other HEI
8.	Are you applying for any other approvals for this research? If so please indicate what they are.	Include University Ethics Committee, Faculty Ethics Committee, MOD
9.	Will your research involve visits to websites that might be associated with extreme, or terrorist, organisations? If so, *The University blocks access to illegal web content, access to blocked web content will be granted for a research project for a maximum of a 6 month period, after which time a review of access must be undertaken before any further period is confirmed*	

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 un-signed word document to RIGO.

1	I confirm that I have discussed the research project with my Supervisor or Head of Department
2	I confirm that I have completed the online Prevent Duty training module.
3	I confirm that the research will not commence until confirmation to do so is received.
4	I confirm that I have completed and will abide by the security-sensitive risk assessment
5	I understand and accept that RIGO will be registering this project on the Universities' security-sensitive research register and will provide this register to the Head of Security and in turn to external agencies where necessary.
6	I confirm I have completed a Data Management Plan
7	I understand that compliance with this policy does not guarantee protection from investigation by authorities in the UK and elsewhere
8.	I confirm that I will abide by the University's Security-sensitive research Policy and all related policies
9.	I understand that websites that might be associated with extreme, or terrorist, organisations may be subject to surveillance by the police. Accessing those sites from university IP addresses might lead to police enquiries.
	Signature:…………………………………………………………………………………. Name:……………..………………………………………………………………………. Department:……………………………………………………………………………. Date form signed:………………………………………………………………………

Security-Sensitive Risk Assessment

Please complete the security-sensitive risk assessment below and once complete send to RIGO (rigo@surrey.ac.uk) alongside the security-sensitive research registration form. Please refer to the security-sensitive research policy, and guide in completing the risk assessment.

The risk descriptors and guidance included below are not exhaustive, and many not apply in all cases, they are intended to be helpful examples only.

Risk Description or Consideration	Impact of Risk – Please state specifically if a Person is at Risk	Scale of Risk	Existing Protocols/Mitigations	Additional Mitigations
State the risk *Examples given below*	*Participant and / or Researcher and / or Organisation*	*Low / Medium / High*	*What is currently in place to mitigate this risk?* *Examples given below*	*Is there anything in addition to the existing protocols that can be done to mitigate this risk?*
Risk of losing or disclosing security sensitive research when stored?			*Guidance:* *Consider physical storage to avoid accidental discovery of security-sensitive materials that could cause alarm/distress* *Consider electronic storage – you are advised to store records/materials on a secure university server (safe store) and will need to contact IT via usersupport@surrey.ac.uk to request such storage* *Consider access restrictions-files should be password protected.*	
Risk of disclosure when sending/transmitting security sensitive			*Guidance: no documents stored in the safe store should be transmitted electronically to a third party.*	

research?				
Risks associated with accessing websites that could be considered security sensitive (this might include facebook groups, etc)			*Guidance: registering the research with RIGO, and awaiting confirmation will provide authorities with assurance, but there remains a risk that visiting these sites may result in police enquiries.* *This will also mean working outside of the University web use policies, and therefore research must not commence until confirmation received.* *The University blocks access to illegal web content, access to blocked web content will be granted for a research project for a maximum of a 6 month period, after which time a review of access must be undertaken before any further period is confirmed. This review should involve the PI, Supervisor or Head of Department, as is appropriate.* .	
Risks associated with failure to appropriately disposal/deletion of security sensitive data			*Guidance: the lead researcher should articulate the plans for data within a data management plan, and refer to RIGO or the Universities' information Compliance Team for advise on timescales for retention/deletion*	
Risks associated with security clearance, and who else may need to have such clearance?				
Risks associated with having untrained staff working on the project.			*What training needs are required for the individuals working on this research, if any? Please indicate for each person what they are.* *Guidance: All researchers working on security-sensitive research should complete the online Prevent Duty training module. (http://www.surrey.ac.uk/currentstudents/it/surreylearn/)*	
Risks to health and safety and wellbeing of			*What steps can be taken to ensure that the work is undertaken in a safe way and that individuals are safeguarded.*	

individuals?			*Guidance: refer to Health and Safety Policy and procedures and also to Children and adults at Risk (safeguarding) policy and procedures (Hyperlink when available)*	
Risks associated with working in other countries (if any)?				
Please continue to add risks				
Please continue to add risks				
Please continue to add risks				

Appendix 3

Guide for Researchers on Conducting Security-sensitive Research

This guidance should be read in conjunction with the Security-sensitive research policy. The guide aims to support researchers in conducting Security-sensitive research and in particular in considering the content of the security-sensitive research risk assessment.

The guide is not exhaustive but highlights considerations that may be relevant to the proposed research, it does not attempt to cover all the issues that may arise when dealing with security-sensitive research.

Risk Assessment

In accordance with the Security-sensitive research Policy, the Lead Researcher is required to produce and maintain a risk assessment. Research must not commence until confirmation has been granted. It is advisable that throughout the research project the risk assessment is reviewed regularly (at least twice a year) and is updated as events change.

Researcher Training Requirements

Before individuals start work on sensitive research, the Lead Researcher and all the researchers involved need to consider any particular training that may be required for themselves or others working on the project to ensure they understand how best to conduct the research in a safe and secure manner.

Researcher Wellbeing

For research that involves the use of material that is extremist or could be used for radicalisation, the risk analysis should explicitly cover the risk to researchers themselves and how those risks can be mitigated. As part of that there should be regular discussions between researchers and the Lead Researcher where progress is discussed. Where the Lead Researcher is the sole researcher on the project, regular progress meetings should be scheduled with their Head of Department.

Where there are concerns regarding the well-being of another colleague those concerns should be escalated immediately to Head of Security.

Security-sensitive Website Access

Researchers who plan to access web sites that might be associated with security-sensitive material must be conscious that such sites may be subject to surveillance by the Police, and that accessing those sites might lead to police enquiries. *This also applies to sites on what is commonly known as the 'dark-web'. Accessing these sites may also affect an individual's application for security clearance in the future.*

The University will block access to certain web content, if access to this content is required as part of the research, then access will be granted, subject to satisfactory completion of the confirmation process. Access will be time-limited, monitored and regularly reviewed, and this should be detailed in the risk assessment.

There are a number of Proscribed[1] organisations where particular care must be taken when researching into these organisations, this is because the organisation commits or participates in acts of terrorism;

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/670599/20171222_Proscription.pdf

prepares for terrorism; promotes or encourages terrorism or is otherwise concerned in terrorism.

Non-Electronic Documentary Data

Paper or other physical documents and media relating to security-sensitive research should ideally be scanned and/or uploaded to the Safe Store. Hard copies should subsequently be securely destroyed.

Data Management, Dissemination and Deletion

All security-sensitive research should be supported by a formal Data Management Plan and that plan should comply with the specific procedures outlined in this policy.

The supervisor or principal investigator should be the data owner and the data owner will normally be responsible for initiating the destruction process. If the supervisor or principal investigator is no longer available, the most relevant Head of Department will be expected to initiate the process.

Researchers should note that the Terrorism Act (2006) and the Counter-Terrorism and Security Act (2015) outlaw the dissemination of terrorist publications if the individual concerned has the intention to encourage or induce others. Publications disseminated for the purposes of a clearly defined research project should not amount to an offence, because the requisite intention is unlikely to be present. However, caution is advised and the dissemination of raw research materials should be avoided where possible.

Researchers must not use personal social media to disseminate raw data and research materials. In particular, researchers must not create hyperlinks to sites used (e.g. sites of any proscribed organisations). Additionally, researchers should adhere to the relevant University policies and guidelines relating to use of University Computers, Internet and Social Media. The outcomes of the research that do not contain raw research materials may be shared via social media and traditional dissemination routes.

Consideration will need to be given to dissemination. For example a PhD Thesis may have two volumes; Volume One (without any security sensitive data) open for academic access and can be put on the internet and library. Volume Two (with security sensitive data) with restricted access.

Funders will need to be made aware that for national security purposes that research material falling with the remit of The Counter-Terrorism and Security Act (2015) may be deleted after the project's final report have been presented. Funders should be informed at the application stage of the Data Management Plan including, for example, proposed deletion dates. Researchers are advised to ensure that funders are content with intended handling of research data, preferably in writing.

Destruction of security-sensitive data must be in accordance with IT Services guidance and the Waste Management policies; where data is stored centrally that will be managed through IT Services. It is the responsibility of the Lead Researcher to provide the instruction to delete.

Storage and Transmission

Any data, files or electronic items used or produced during projects that fall under this Policy must be stored appropriately. At the University of Surrey, this will normally be the Safe Store as provided by IT.

No data relating to work covered by this Policy should be stored on local computers or external storage devices. Please note conclusions from the research that do not include security-sensitive raw data, can be stored locally.

For collaborative projects where data is being stored at a third party organisation, written confirmation as to their storage arrangements must be obtained. These should be included as part of the security-sensitive risk assessment, and will be reviewed as part of the procedures set out in the Security-sensitive research Policy. .

In the instance of collaborative research projects with researchers at other institutions in the UK or abroad, the sharing of documents may be necessary. Where necessary this requirement must be identified during the confirmation process and a suitable mechanism articulated in the risk assessment. Under no circumstances should any documents associated with sensitive research be transmitted using conventional, unprotected channels (e.g. unsanctioned internet email).

Researchers are strongly advised to avoid physically transporting materials connected to sensitive research projects. If it is unavoidable, the approach to transporting the materials must be described in the risk assessment.

IT Facilities

Once confirmation has been granted, researchers must only use the University IT facilities agreed in the risk assessment to carry out their research. This will ensure these activities can be identified as a legitimate part of their research. No other University or non-University IT facilities may be used (e.g. home computers or broadband.)