Security-sensitive Research Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Research and Innovation - PVC, Research and Innovation Executive Board
Is the Procedure for internal use only (Non-disclosable) ?	Disclosable
Associated Policy Statements:	Our Data - Chief Operating Officer Our Partners and Reputation - Vice-President Global Our Safety - Chief Operating Officer Our Students - Chief Student Officer
Authorised Owner:	Head of Assurance (Research, Innovation and Impact)
Authorised Co-Ordinator:	Director of Research Innovation and Impact
Effective date:	July 2025
Due date for full review:	July 2028
Sub- documentation:	**Security Sensitive Checklist** **Security Sensitive Research Registration Form** **Security Sensitive Research Risk Assessment**

Approval History

Version	Reason for review	Approval Route	Date
1.00	To move policy into procedure template	URIC Executive Board	May 2025 July 2025

1. Purpose

1.1. Universities play a vital role in carrying out research on issues where security-sensitive, radical or extreme material is relevant. The University of Surrey does not intend to prevent or restrict such research but rather to ensure processes are in place and risks are understood and managed. Through this procedure, 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, whilst complying with relevant legislation.

1.2. Carrying out security-sensitive research may trigger a level of personal risk to the researcher that cannot be mitigated by the University. Whilst compliance with this procedure does not guarantee protection from investigation or prosecution by national or international authorities, or from action taken by enforcement or security agencies outside of the United Kingdom, it does mean that the University can aim to support the researcher to the best of its ability.

1.3. Specifically, but not exclusively, the procedure 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.

1.4. Adherence to this procedure 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.

1.5. 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*"

2. Scope and Exceptions to the Procedure

2.1.This Procedure covers Security-Sensitive Research as defined in the Definitions section (3.1) and includes research activities and related activities such as providing consultancy, innovation, and commercial and analytical. It excludes teaching.

2.2. The Procedure applies to the following groups of people undertaking Security-Sensitive Research

- 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
- Undergraduate and postgraduate students (both taught and research), whether registered here or on temporary placement
- Undergraduate and Master's level research should not normally involve accessing security-sensitive materials described above but where this is required by the school, the procedure will apply.

2.3.The procedure covers activities undertaken in the UK or in any overseas location and includes research that may be led by another Institution but where a University of Surrey researcher is contributing to research.

2.4. 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 those relating to collecting and holding sensitive data.

2.5. This procedure 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 and excludes considerations of confidentiality or non-disclosure that may be required under law or as part of contractual arrangements with funders

3. Definitions and Terminology

3.1. **Security-sensitive Research**, for the purpose of this procedure, relates to research involving one or more of the categories 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 Terrorism Act 2006

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 radicalization

iii) Research or materials used for research projects commissioned by the military or under an EU security call and require 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.

4. Procedural Principles

4.1. Principles

4.1.1 Ensuring Researcher Well Being: Alongside the Universities Our Safety Policy Statement and Ethics procedure, this procedure is designed to ensure that those involved in security-sensitive research can conduct that work safely.

4.1.2 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.

4.1.3 A Risk Based Approach to Security-sensitive Research: This procedure 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 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.

4.1.4 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.

4.1.5 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. The Identification and Confirmation procedures are described in the workflow diagram included as Appendix 1.

4.2. Procedures

4.2.1 **Identification**

The Lead Researcher (usually Supervisor or Principal Investigator) is responsible for assessing whether the research is covered by this procedure. If the Research is not being led by the University an alternative" Surrey Principal Investigator" 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 procedure.

Researchers are encouraged to discuss potentially Security-Sensitive Research at the earliest point: students with their supervisor, members of staff with their Head of School. Any special provisions, facilities or resources such as access to security sensitive websites that may contravene the acceptable use procedure and be inaccessible due to the university's web filtering processes or secure storage of materials, must be identified as early as possible and agreed with the relevant departments, including but not limited to, IT Services and Estates and Facilities. Where there are likely to be cost implications to conducting the research, this must be identified and agreed before submission of the grant or contract award.

4.2.2 **Registration**

Research that is identified as within the Security-Sensitive Research procedure remit must be registered and undergo the confirmation process (4.2.3) before the research commences.

A Security-Sensitive Risk Assessment (Appendix 2) must also be completed, indicating the main risks and how these will be mitigated. Proper consideration should be given when completing the risk assessment of the University's policies and procedures that may be relevant, including but not limited to IT, procurement, health and safety, insurance, governance and travel. The Security-Sensitive Research Registration form and Risk Assessment must be sent to Assurance at the email address indicated on the forms.

If 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".

4.2.3 **Confirmation Process**

The Security-Sensitive Research Registration Form and Risk Assessment will be initially reviewed by Assurance for completeness and to identify all potentially Security-Sensitive issues that require expert review.

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

Assurance 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 School or Supervisor for academic staff and research students respectively.

If the confirmation process identifies significant reputational risks or infrastructure limitations, the decision to grant confirmation will be referred to the Pro-Vice-Chancellor Research & Innovation (PVCRI). The PVCRI will inform Assurance by email and if applicable, 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 PVCRI within one month of receipt of the refusal email. The basis of the appeal may only be made on the grounds of (i) procedural irregularity and/or (ii) equality.

Any change in scope, documents, or research design of 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 Assurance and where an ethical review was also applicable it will be considered as an amendment and must obtain the necessary approval.

4.2.4 **Security-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 Security-Sensitive Research Register to be maintained by Assurance. Security-Sensitive Registration Forms and Risk Assessments will be held on the University secure network. An updated copy of the University Security Sensitive Research Register will be issued to the Head of Security after every complete Confirmation process or at least every 6 months.

4.3. Handling 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 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 procedure 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 from Assurance. 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.

4.4. Handling 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 Assurance will co-ordinate with the Head of Security in considering and granting requests and for ensuring access is chaperoned.

4.5. Discovering Security-sensitive materials

Any member of staff or student who becomes 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.

4.6. Breach of the Procedure

Intentional breaches of this procedure will be considered as research misconduct and investigated through the "Code of Practice on Handling Allegations of Research Misconduct" Code of Practice

5. Governance Requirements

5.1. **Implementation: Communication Plan**

5.1.1. The University's ethics guidance webpages to be updated and added to with security-sensitive specific details

5.1.2. All forms and guidance relating to this procedure will be made freely available online on the Assurance Research Integrity pages.

5.2. Implementation: Training Plan

5.2.1. Broad University level training: Provided to all staff via the SurreyLearn compulsory modules: Prevent Duty module

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

- Their specific duties under this procedure
- Handling security-sensitive materials
- Handling and escalating concerns or enquiries about security-sensitive research

5.3. **Review**

5.3.1. This procedure will be reviewed every three years or sooner following any material legislative changes

5.4. **Legislative Context and Higher Education Sector Guidance or Requirements**

5.4.1. Legislation

Counter - Terrorism and Security Act 2015
Official Secrets Act 1989
Terrorism Act 2006
Data Protection Act 2018
Health and Safety at Work Act 1974
Export Control Act 2002
Equality Act 2010
Management of Health and Safety Regulations 1999

5.4.2. Guidance

Universities UK Guidance
https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/oversight-security-sensitive-research

'Prevent Duty Guidance for higher education institutions in England and Wales', dated July 2015, available at
https://www.gov.uk/government/publications/prevent-duty-guidance-england-scotland-and-wales-2015/prevent-duty-guidance-for-higher-education-institutions-in-england-and-wales-2015

5.5. **Sustainability**

5.5.1. This procedure requires the completion of online forms. There is a small amount of energy use, no waste and no use of materials

5.5.2. This procedure is not expected to have negative impact on the 17 United Nations sustainable development goals. There is a positive contribution to "Peace, Justice and Strong Institutions" by ensuring the University documents all research involving the military and research into terrorism and radicalization

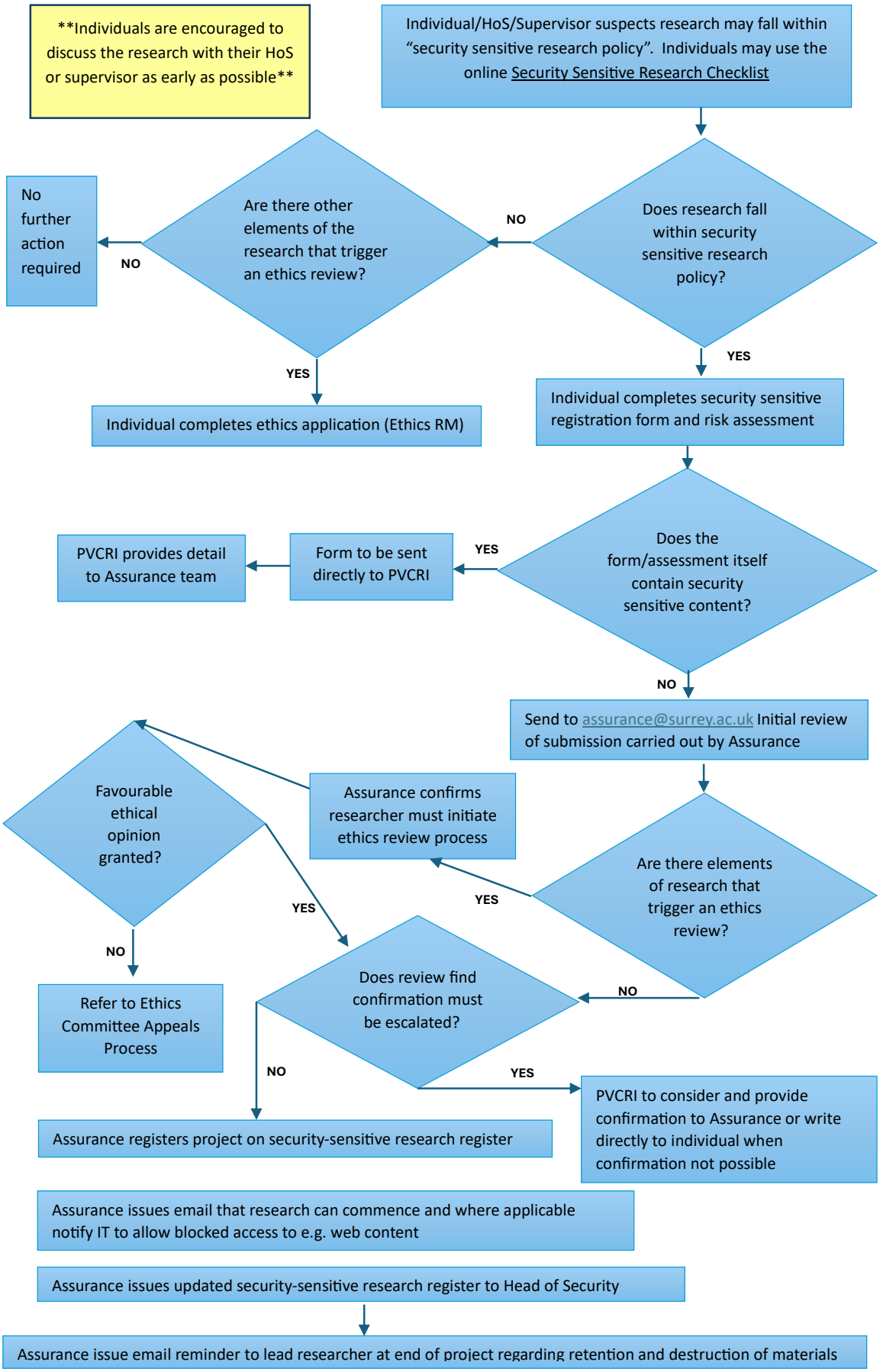
6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on **28/04/2025** and is held by the Authorised Co-ordinator.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Request EB Approval (Y/N)**	**Date**	**Name of Contact**
Governance	Emailed version 16th April		12/05/25	Kelley Padley
H&S	Emailed version 16th April	N	07/05/2025	Matt Purcell, Director of Health and Safety
Sustainability	Emailed version 16th April			Martin Wyles
Academic Freedom / Freedom of Speech	Emailed version 16th April		08/05/2025	Abi Bradbeer
Our Partners and Reputation	Emailed version 1st May			Patrick Degg
Our Students	Emailed version 1st May			Emma Rowsell
Our Data				Ewan Robson
Chief Operating Officer	Emailed version 1st May			Will Davies
Chief Student Officer	Emailed version 1st May			Emma Rowsell

Appendix 1 – Security-sensitive Research workflow



Appendix 2: Security Sensitive Research Checklist, Registration Form and Risk Assessment

Security Sensitive Checklist

This checklist is an aid to help researchers consider if their research falls under the requirements of the Security Sensitive Research Procedure.

Students should complete this checklist with their supervisor.

Security-Sensitive Research Criteria	Yes or No
1. Does the research involve research or materials that are covered by the Official Secrets Act 1989, the Terrorism Act 2006 and/or the Counter Terrorism Act 2015?	
2. Does the research 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? (definitions below)	
3. Has the research been commissioned by the UK Ministry of Defence, the Secret Intelligence Service (MI6), the Security Service (MI5) or another UK government body 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 any non-UK military or security services?	
6. Are there any other reasons why the research may be considered security-sensitive?	

If you have answered "yes" to any of the questions, the research is likely to fall within the Security Sensitive Research Procedure and you are required to follow the Security Sensitive research registration and confirmation process.

If you are unsure than you are advised to seek advice from the Assurance Team (assurance@surrey.ac.uk). Please note that specific details of the research and documents should not be sent. If you feel it is necessary to provide these, please direct your enquiry to the Pro-Vice-Chancellor (Research & Innovation) PVCRI.

Definitions:

Extremism is defined in the 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 member 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 of 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.
Security Sensitive Research Registration Form

Once complete, please send this form to the Assurance Team assurance@Surrey.ac.uk along with the completed Risk Assessment.

Security Sensitive Registration Form

Section A: Security-Sensitive Research Criteria *Please confirm the criteria that has triggered this registration form*	**Yes or No**
1. Does the research involve research or materials that are covered by the Official Secrets Act 1989, the Terrorism Act 2006 and/or the Counter Terrorism Act 2015?	
2. Does the research 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? (definitions below)	
3. Has the research been commissioned by the UK Ministry of Defence, the Secret Intelligence Service (MI6), the Security Service (MI5) or another UK government body 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 any non-UK military or security services?	
6. Are there any other reasons why the research may be considered security-sensitive?	
Section B: Basic Project Details *Please complete this section as fully as possible. If you are completing on ethics and governance application at the same time this section can be left blank and the two applications submitted together.*	
7. Title of Project	
8. Worktribe or finance project code	
9. Start and end dates for project	
10. Name of person submitting this form Lead Research, if different	
11. Is this project a collaboration with an external organisation? Please indicate which is the lead organisation	

12. Is the research covered by a UK or other government security classification? Please give details

13. Where will the research be carried out?

14. Are you applying for any other approvals (University Ethics Committee, MODREC etc.) for this research? Please provide details.

15. Will your research involve visits to websites that might be associated with extreme or terrorist organisations?
The University blocks access to illegal web content. Access can be granted for a research project for a maximum of 6 months, after which a review of access is undertaken.

Section C: Declarations

Please read each declaration and confirm your agreement by adding a signature below. Electronic signatures are acceptable.

- I confirm that I have discussed the research project with my supervisor or Head of School.
- I confirm that I have completed the online Prevent Duty training module.
- I confirm that the research will not commence until confirmation to do so if received.
- I confirm that I have completed and will abide by the security-sensitive risk assessment.
- I understand and accept that the Assurance Team will be registering this project on the University's security-sensitive research register and will provide this register to the Head of Security and to external agencies where necessary.
- I confirm I have completed a data management plan
- I understand that compliance with the Security Sensitive Research Procedure does not guarantee project from investigation by authorities in the UK and elsewhere.
- I confirm I will abide by the Security Sensitive Research Procedure and all related policies and procedures.
- 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	
Date	
School	

Security Sensitive Research Risk Assessment

Please complete this risk assessment and send to the Assurance Team assurance@surrey.ac.uk along with the Security Sensitive Research Registration Form. Please refer to the Security Sensitive Research Procedure and guide when completing the Risk Assessment.

As part of your Security-Sensitive Research application you must assess any risk arising out of your proposed research. Your risk assessment should demonstrate that you have considered the risk of harm to yourself and others i.e. the research team, participants and anyone not directly involved for whom the research could have a negative impact.

Please note, the table below provides examples but is not definitive.

Identified Risk	**Likelihood**	**Potential Impact / Outcome**	**Potential Severity of Outcome**	**Risk Management / Mitigating measures**
e.g. Data loss				
e.g. distress/upset to research team on viewing extremist material				
e.g. Risks associated with accessing websites that contain extremist material				
e.g. adverse publicity				