Security Sensitive Research Policy

Policy No: **P2122-200**
Effective Date: 12/10/2021
Last Revised: 12/10/2021
Review Interval: Biennial
Review Date: October 2023
Approval Body: University Research Impact & Innovation Committee
University Research Integrity: Ethics & Governance Committee
Senate.

Policy Owner: Research Engagement & Innovation Services (REIS),
Academic Services (Data Management)

Policy Author: Anjana Choudhuri (a.choudhuri@swansea.ac.uk)
Alexander Roberts (a.roberts@swansea.ac.uk)

Related Policies

1. Research Integrity: A Policy Framework on Research Ethics and Governance
2. Health and Safety Policy
3. Prevent Policy

Policy History

Revision Date	Author	Description
N/A	As above	Version 1

Contents

1	Introduction
	Transparency and openness are integral to the success of research and innovation as without this the benefits of such activities cannot be fully realised. This requirement should, however, be balanced with the need to safeguard information whilst sharing knowledge. It is therefore a requirement of UK Research & Innovation (UKRI), that organisations have in place a robust information security management system that ensures that access to sensitive data and information is appropriately managed. The aim of this Policy is to provide guidance to researchers regarding assessing and mitigating issues in relation to undertaking research that is defined as 'security sensitive'. Such research may involve activity that may put the institution, its staff, or students at risk of harm, or of causing a threat to national security. Likewise, such research may be on security sensitive, radical, or extreme material. If circulated carelessly, security sensitive material can sometimes be open to misinterpretation by the authorities and can put researchers in danger of arrest and prosecution under counter-terrorism legislation. It is not the intention of this policy to prevent or restrict such research, but to enable researchers, and support services to understand and manage risks associated with such activity. Researchers are expected to exercise an element of caution and judgement whilst considering accessing any material that could be categorised as: ▪ Extremist: material that results from collecting information from websites of extremist organisations ▪ Terrorist: material gained through gathering content on actual or potential terrorist methods ▪ Radical: material obtained by liaising with groups which seek to persuade young people to adopt extreme political, religious, or social views ▪ Prohibited or Government information: information on national security, official secrets act, military intelligence, measures to combat terrorism, extremism, or radicalisation etc. unless the research has been commissioned or sponsored by Government. Adherence to this policy will assist researchers and the University to demonstrate to external authorities that actions of the researcher(s) were part of a legitimate research activity. 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, students, and the University. Specifically, but not exclusively, this policy aims to ensure compliance with the Counter-Terrorism and Security Act2015,The Prevent Duty guidance for Higher Education England and Wales https://www.gov.uk/government/publications/prevent-duty-guidance and the research funder requirements of Trusted Research The procedures laid out in the policy follow the recommendations of Universities UK guidance on oversight of security sensitive research materials and the guidance provided by University UK and UK Research & Innovation . Procedures for independently registering projects that intend to create and/or store such material, through research ethics processes, are recommended in this guidance. This Policy does not replace the requirement for other approvals that projects may have 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.

2	**Scope**
	This Policy covers research and related activities i.e., fundraising, providing consultancy, innovation, commercial and analytical services and the setting up and running of University spin-out companies. The Policy applies to the following groups of people if 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 to work on the University campus 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 Swansea University 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 with regards to collecting and holding sensitive data. **Note:** Compliance with the policy does not guarantee protection from investigation or prosecution by external authorities. In particular, the process may not protect individuals from actions taken by other country's security or legal agencies.
3	**Equality Impact assessment**
	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
4	**Purpose**
4.1	**Legislative context**
	The relevant sections of legislation that relate to the storage and circulation of security sensitive material are: • Section 58 of the Terrorism Act 2000 as amended by sections 3 and 7 of the Counterterrorism and Border Security Act 2019 • Sections 1, 2 and 3 of the Terrorism Act 2006 • Section 2 of the Terrorism Act 2006 as amended by sections 5(6) and 5(7) of the Counterterrorism and Border Security Act 2019 Relevant legislation can be read in full using the following links: • Health and Safety at Work Act 1974 • Official Secrets Act 1989 • Data Protection Act 1998 • Export Control Act 2002 • Terrorism Act 2006 • Equality Act 2010

	• Counterterrorism and Security Act 2015
4.2	**Health & Safety Implications**
	This policy supports the principles articulated in the Health and Safety Policy and apply to: **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 - both physically and mentally (i.e., when exposed to material which may compromise mental wellbeing).
4.3	**Governance Requirements**
	University's Involvement in Security-sensitive Research Procedures for dealing with security-sensitive research should be embedded in research ethics approval processes. The University Research Integrity Ethics & Governance Committee (URIEGC) reporting to University Senate & Council, has the overall responsibility for ensuring that all security sensitive research undertaken within the University premises is monitored in accordance with UK Govt guidelines. This body is also responsible for advising on policies and strategies for ethics and governance. The responsibility for the ethical review of individual security sensitive research projects is devolved to Faculty/School Research Ethics & Governance Committees (SREGCs). Trained staff within IT security or the Prevent Team can assist the Faculty/School Ethics committees on decisions in relation to security sensitive research. The Faculty/School committees provide regular reports to the University Research Integrity Ethics & Governance Committee (URIEGC) through a standing agenda item. The University committee is also provided with a register of approved security sensitive projects. This register is maintained by Research Engagement and Innovation Services (REIS) Department. Research that involves accessing security sensitive materials requires ethical approval at Faculty/School level as a minimum, and potentially at University Research Integrity Ethics & Governance Committee level where SREGCs do not feel able to approve such projects without a University wide view. **Note: All security-sensitive research must be identified so that it can be subjected to Confirmation and Registration before the research begins and to aid authorities with external enquiries.**
4.4	**Responsibilities**
	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 reregistering 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 Faculty/School/Associate Deans of Research/Head of Departments** • Heads of Faculty/School Department and Associate Deans for Research 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 research. **Research Engagement & Innovation Services** • 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, and seek legal advice where necessary. • To manage and co-ordinate the implementation of this Policy and to ensure it is kept updated. To maintain a register of all security-sensitive research being undertaken and provide this to the Head of Security. **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. **University security and legal function** Campus security, Planning and Strategic Projects Unit security, and legal assurance team **Information Security function** Research Data Management, IT Services, Cybersecurity, and Information Security
5	**Managing information & Knowledge sharing**
5.1.	**A Risk Based approach to Security-sensitive Research** This Policy is not designed to stop security sensitive research or restrict academic freedom but to ensure that any risks associated with such research are well understood and 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 will be undertaken for any such work. Prior to the commencement of any research into security-sensitive, radical or extreme material, permission by the University must be granted. The process must include a risk assessment that has been reviewed by the Faculty/School Research Ethics and Governance committee that includes input from the appropriate University security and legal teams Alongside a cyber security culture achieved through the development of cyber controls and security awareness, a training program that includes well publicised guidance for staff and students is essential for reducing the risks of cyber security.
5.2	**Safe Storage, Access, and Transmission of security-sensitive Material**

	UKRI advices that sensitive data must be secured stored and where a shared platform is used for information exchange, data should be logically separated into different locations so that it is only accessible by authorised individuals. 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 law enforcement agencies who may require access in connection with a criminal investigation. Access to sensitive data should only be given to individuals with a clear requirement for access and for the duration that such an access is required. Access by any other agencies would be subject to the possession of a relevant warrant, or equivalent. The University has put systems and procedures in place that are aligned with the Universities UK guidance for the storage of security-sensitive research material, see Universities UK: Oversight of security-sensitive research material in UK universities. Please refer to the Information Security and IT Services policies and procedures below: Digital-Acceptable-Use-Policy-V1.0-October-2019.pdf (swansea.ac.uk) Note: All research that produces security-sensitive research material must have a data storage access and disposal plan that has been agreed with the Research Data Management Team in place before research can commence
5.3	**Safe Disposal** Security-sensitive material must be disseminated or disposed of in accordance with security protocol or data protection requirements as stipulated in the information security and IT services guidelines Information Security - Swansea University and policies Digital-Acceptable-Use-Policy-V1.0-October-2019.pdf (swansea.ac.uk) Security sensitive material must only be stored for as long as is required to conduct the research and comply with any legal requirement or best practice guidance concerning maintaining original data. Where funders require security sensitive research data to be archived on any external system and/or made openly available, permission and guidance must be sought via the Research Data Management Team or the Research Integrity Manager, before any such data is made available openly. Note: All research that produces security-sensitive research material must have a data storage access and disposal plan that has been agreed with the Research Data Management Team in place before research can commence
6	**Procedure**
6.1	*The Identification and Confirmation procedures are described in the workflow diagram included in Annex 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 Swansea University an alternative "Swansea Principal Investigator" at the University must be identified. The security-sensitive research checklist (Appendix 2) is available to Swansea University staff if they are unsure whether 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/Principal Investigator.**

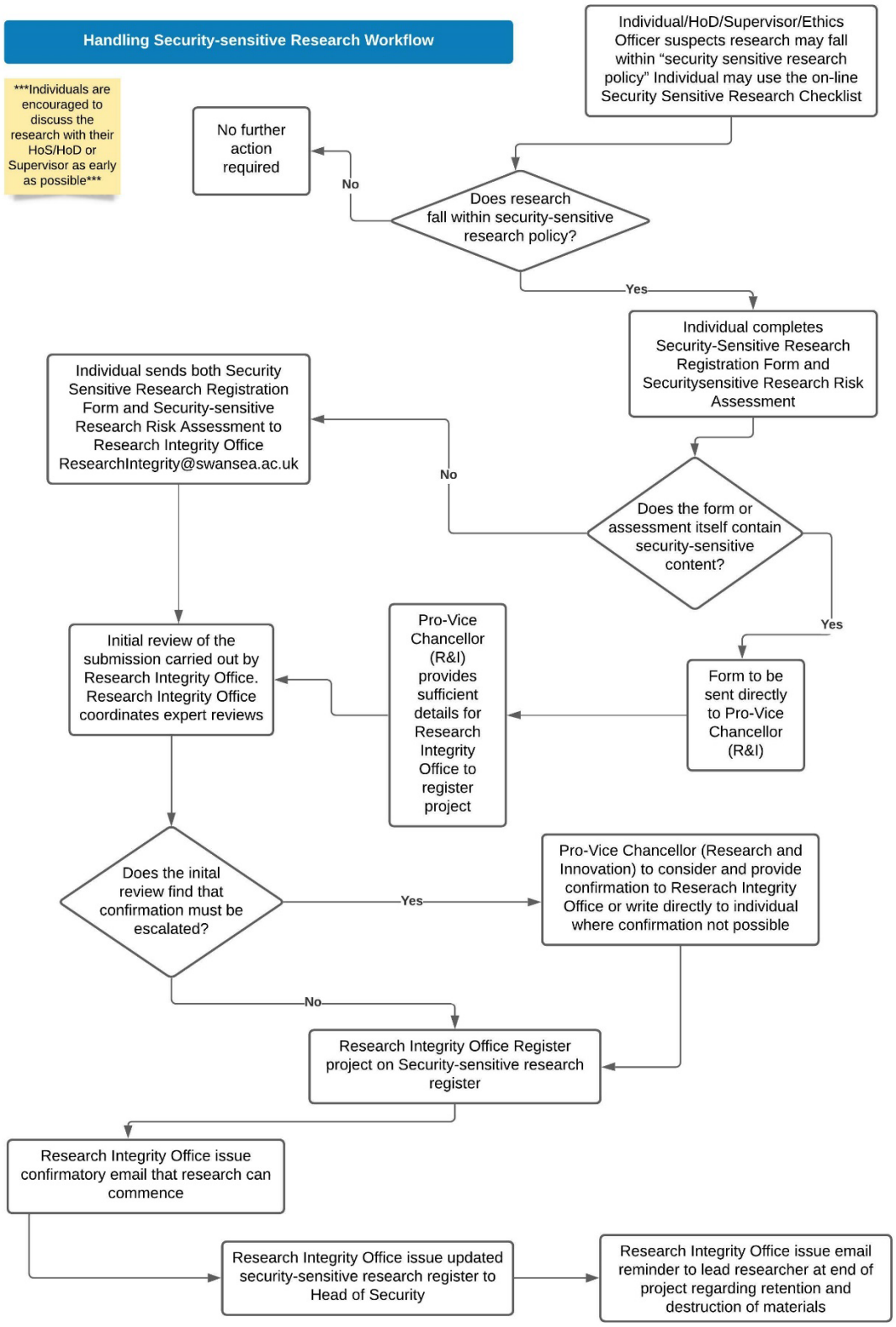
	Any special provisions, facilities, or resources such as access to security sensitive web sites that may contravene the Digital-Acceptable-Use-Policy-V1.0-October-2019.pdf (swansea.ac.uk) or secure storage of materials, must be identified as early as possible and agreed with the relevant department, including but not limited to IT Services and Estates and Facilities. Where there are likely to be cost implications for conducting the research, discussions must be had before submission of the grant or contract award.
6.2	**Registration** 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. The security-sensitive research registration form and risk assessment must be submitted by the Faculty/School Research Ethics committee and an email confirmation sent to researchintegrity@swansea.ac.uk or 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 Swansea University ethics review process is described in the Framework document on for Research Integrity: Ethics & Governance UWS Ethics Committee (swansea.ac.uk)
6.3	**Confirmation Process** The security-sensitive research registration form and risk assessment will be initially reviewed by the Faculty/School Research Ethics & Governance committee for completeness and to identify all potentially security sensitive issues that require expert review. If the Faculty/School Research Ethics committee is unable to decide on an application or require an expert review of the risk assessment, then they will contact the Research Integrity Manager via email researchintegrity@swansea.ac.uk The Research Integrity Manager will co-ordinate expert reviews and risk assessment liaising with appropriate personnel and policy holders from across the University. If the expert reviewers require additional information or changes to procedures or risk mitigation before confirmation to commence research can be granted, they will feedback the suggestions to the Chair of the Faculty/School Research Ethics & Governance committee who will verify the requirements with the Lead Researcher. On completion of the Confirmation process, the Chair of the School Research Ethics & Governance committee will issue a confirmatory email to the Lead Researcher informing them that the research could commence. If the confirmation process identifies significant reputational risks or infrastructure limitations, the decision to grant confirmation will be referred to the Chair of the University Research Integrity Ethics & Governance committee (URIEGC) who is also the Pro Vice Chancellor (Research and Innovation). The Chair of URIEGC will inform the Chair of Faculty/School Research Ethics & Governance committee by email the decision and in the event of a refusal the grounds for the decision.

	The Lead Researcher may appeal the decision in writing to the Chair of URIEGC 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 the Faculty/School Research Ethics & Governance committee and where an ethical review was also applicable it will be considered as an amendment in accordance the Framework for Research Integrity: Ethics & Governance. UWS Ethics Committee (swansea.ac.uk)
6.4	**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-wide security-sensitive research register maintained online. The 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.
6.5	**Handling Security-sensitive research 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 Swansea 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 agreed with the Research Data Management team 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 and agreed with the Research Data Management Team. Where the sharing of raw data beyond the Swansea 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 to a secure server folder and hard copies should subsequently be securely destroyed.
6.6	**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 the Research Integrity Compliance Office will co-ordinate with the Head of Security in considering and granting requests and for ensuring access is chaperoned.
6.7	**Discovering Security-sensitive research materials**

	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 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.
6.8	**Breach of the Policy** Intentional breaches of this policy will be considered as an act of research misconduct and investigated through the "Code of Practice on Handling Allegations of Research Misconduct". Please raise any breaches to this policy or misconduct allegation by mailto: researchmisonduct@swansea.ac.uk
7	**Implementation / Communication Plan**
7.1	**Training** The University has a responsibility to provide to all university-based internet users, information about the dangers of accessing and storing security sensitive material. By providing clear advice and research-specific mechanisms, risk and difficulties arising from individuals accessing sensitive material for legitimate purposes can be minimised. Broad University level training will be: • Provided to all staff via the compulsory modules: Prevent Duty module • In-depth Training for those carrying out expert reviews or likely to advise staff and students on requirements under the Policy will include members of the University and Faculty/School Research Integrity Ethics & Governance Committees, University Governance & Legal, IT services, Research Integrity Compliance and Campus Security. A training programme will be made available to researchers working in this area of research and will include: **1.** Their specific duties under the Policy **2.** Handling, storing, disseminating, and disposing security-sensitive materials **3.** Handling and escalating concerns or enquiries about security-sensitive research The University's ethics guidance and due diligence webpages will be updated and added to with security-sensitive specific details. All forms and guidance relating to this policy will be made freely available online.
8	**Exceptions to this Policy**
	Any activities outside of Section 2
9	**Supporting Documentation**
9.1	Swansea University Internal Supporting Documentation: • Security-sensitive research checklist • Security-sensitive research registration form • Security-sensitive research risk assessment • Security-sensitive research Workflow Diagram • Guide for Researchers on Conducting security-sensitive research

9.2	**External Supporting Documentation** *Universities UK guidance, available at*; http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/oversight-ofsecurity-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. '*Managing Risks in Internationalisation – security related issues'* Universities UK; dated October 2020, available at; Managing risks in Internationalisation: Security related issues (universitiesuk.ac.uk) '*Trusted Research – Guidance for Academia'*; National Cyber Security Centre, Centre for Protection of National Infrastructure; dated March 2021 Trusted Research Guidance for Academia.pdf (cpni.gov.uk)
9.3	**Acknowledgements** This guide was authored in reference to other guides and policies available from UK Research & Innovation (UKRI), Universities UK (UUK), City, University of London, University of Huddersfield, and the University of Surrey.

Appendix [1]: Handling Security-sensitive Research Workflow



Appendix [2]: 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?	
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 military or security services?	
4. Has the research been commissioned under an EU Security Call?	
5. Does the work require security clearances to undertake the research?	
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 RIO (Research Integrity Office)

Please note specific details of the security sensitive research, and attachments should not be sent to RIO, 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.

Appendix [3]: 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 researchintegrity@swansea.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 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?	
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 military or security services?	
4. Has the research been commissioned under an EU Security Call?	
5. Does the work require security clearances to undertake the research?	
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
1.	Title of project	
2.	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 Swansea, 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

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 to the Research Integrity Office at researchintegrity@swansea.ac.uk

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 RGO 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
	Signature: …… Name: …… Faculty/School/Department: …… Date form signed: ……

Appendix [4]: Security-Sensitive Risk Assessment

Please complete the security-sensitive risk assessment below and once complete send to the Research Integrity Office (researchintegrity@swansea.ac.uk) alongside the security-sensitive research registration form above. Please refer to the security-sensitive research policy, and guide below 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 and will need to contact IT via customerservices@swansea.ac.uk to request such storage Consider access restrictions-files should be password protected.	
Risk of disclosure when sending/transmitting security sensitive research?			Guidance: no documents should be transmitted electronically to a third party.	
Risks associated with accessing websites that			Guidance: registering the research with RIO, and awaiting confirmation will provide	

could be considered security sensitive (this might include Facebook groups, etc)			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.	
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 RIO or the Universities' information Compliance Team for advice 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.	
Risks to health and safety and wellbeing of individuals?			What steps can be taken to ensure that the work is undertaken in a safe way and that individuals are safeguarded. 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)?				

Appendix [5]: 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 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 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. There are several 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; 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 secure University drive. Hard copies should subsequently be securely destroyed.

[1] https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

Data Management, Dissemination and Deletion

All security-sensitive research should be supported by a formal Data Management Plan that has been agreed with the Research Data Management Team 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 Counterterrorism 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 Counterterrorism 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.

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.

Glossary of Terms

	Definitions
	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. Accessing websites relating to terrorism, radicalisation and/or downloading material considered 'extremist' (this is defined as, 'vocal and active opposition to fundamental human values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs' in the Counter Terrorism and Security Act (2015)) iii) Research or materials used for research projects commissioned by the military or under an EU security call. iv) Research that concerns terrorist or extreme groups e.g., animal rights v) Research that involves IT encryption design for public bodies or business vi) Research into proscribed organisations vii) Research that involves primary criminal or illegal activity viii) Internationalised research with overseas partners in countries where legislative and regulatory requirements are not aligned with those in the UK ix) Research that involves anything else which the University considers as putting researcher(s) at risk **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 human 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.