Checklist, Registration Form and Risk Assessment for Security Sensitive Research (SSR)

Revision 1.1 (May 2023)

Contents

[1. Security Sensitive Research Checklist 2](#_Toc135226959)

[2. Security‐Sensitive Research Registration Form 4](#_Toc135226960)

[3. Security‐Sensitive Risk Assessment 6](#_Toc135226961)

[4. Guide for Researchers on Conducting Security-Sensitive Research 9](#_Toc135226962)

## 1. Security Sensitive Research Checklist

|  |  |
| --- | --- |
| **Security Sensitive Research Criteria** | **Add a “X” to all that apply** |
| 1. Does the work involve research or materials that are covered by the Official Secrets Act 1989 and the Terrorism Act 2006?
 |  |
| 1. Does the work involve research into extremism or radicalisation and/or involve materials that could be considered ‘extremist’ or which could be used for the purpose of radicalisation?
 |  |
| 1. Has the research been commissioned by the military (including agencies that are directly funded by the military), police or security services? Or is the proposed research of potential military or security interest?

For example, if your research is funded by the Ministry of Defence (MoD), one if its agencies, such as the Defence Science and Technology Laboratory (DSTL) then it falls within this definition. Similarly, if your research is being entered into a competition, such as the Defence and Security Accelerator (DASA) themed competitions, or similar then it also falls within this definition. |  |
| 1. Has the research been commissioned under an EU Security Call?
 |  |
| 1. Does the work require security clearances to undertake the research?
 |  |
| 1. Are there any other aspects not covered by the criteria above that could make the research security-sensitive?
 |  |

**If you tick any of the above, the proposed research is highly likely to fall within the security-sensitive research policy and you are required to follow the security-sensitive research registration and confirmation process.** If you are unsure, then you are advised to seek general advice from the Research Integrity Office via researchintegrity@swansea.ac.uk.

**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.

## 2. 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 Research Integrity Office (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?
 |  |
| 1. Does the work involve research into extremism or radicalisation and/or involve materials that could be considered ‘extremist’ or which could be used for the purpose of radicalisation?
 |  |
| 1. Has the research been commissioned by the military (including agencies that are directly funded by the military), police or security services? Or is the proposed research of potential military or security interest?

For example, if your research is funded by the Ministry of Defence (MoD), one if its agencies, such as the Defence Science and Technology Laboratory (DSTL) then it falls within this definition. Similarly, if your research is being entered into a competition, such as the Defence and Security Accelerator (DASA) themed competitions, or similar then it also falls within this definition. |  |
| 1. Has the research been commissioned under an EU Security Call?
 |  |
| 1. Does the work require security clearances to undertake the research?
 |  |
| 1. Are there any other aspects not covered by the criteria above that could make the research security-sensitive?
 |  |

|  |  |
| --- | --- |
| **Section B – Basic Project Details** Please complete this next section as fully as possible. If you are completing an ethics application also, Section B can be left blank and reference made to a completed Ethics Application ID | Guidance |
|  | Title of project |  |
|  | UNCLE ref: and/orFinance Project Code: |  |
|  | Start and End dates for the Project |  |
|  | Name of person submitting form | Main contact for any correspondence |
|  | 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 |
|  | Is the research covered by a UK or other government security classification? If so please give details. |  |
|  | 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 |
|  | 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 alongside the unsigned word document to Research Integrity Office (researchintegrity@swansea.ac.uk) |
|  | I confirm that I have discussed the research project with my:Supervisor or Head of Department / Associate Dean, Research, Innovation, and Impact/ Head of Faculty (Please delete as appropriate) |
|  | 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 is received. |
|  | I confirm that I have completed and will abide by the security-sensitive risk assessment |
|  | I understand and accept that the Research Integrity Office 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. |
|  | I confirm I have completed a Data Management Plan |
|  | I understand that compliance with this policy does not guarantee protection from investigation by authorities in the UK and elsewhere |
|  | I confirm that I will abide by the University’s Security-sensitive research Policy and all related policies |
|  | Signature: ……………………………………………………………………………………. Name: ……………..…………………………………………………………………………. Department: …………………………………………………………………………………. Date form signed: …………………………………………………………………………… |

## 3. Security‐Sensitive Risk Assessment

Please complete the security-sensitive risk assessment below and once complete send to Research Integrity Office (researchintegrity@swansea.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 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 stored in the safe store should be transmitted electronically to a third party. |  |
| Risks associated with accessing websites that could be considered security sensitive (this might include facebook groups, etc) |  |  | *Guidance: registering the research with RESEARCH INTEGRITY OFFICE (RESEARCHINTEGRITY@SWANSEA.AC.UK), 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.* |  |
| 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 RESEARCH INTEGRITY OFFICE (RESEARCHINTEGRITY@SWANSEA.AC.UK) 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. (*[Prevent duty training: Learn how to support people susceptible to radicalisation | Prevent duty training (support-people-vulnerable-to-radicalisation.service.gov.uk)](https://www.support-people-vulnerable-to-radicalisation.service.gov.uk/portal#awareness-course) |  |
| 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*** [swansea-university-safeguarding-policy.pdf](https://www.swansea.ac.uk/media/swansea-university-safeguarding-policy.pdf) |  |
| Risks associated with working in other countries (if any)? |  |  |  |  |
| Please continue to add risks |  |  |  |  |
| Please continue to add risks |  |  |  |  |
| Please continue to add risks |  |  |  |  |

## 4. 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. There are a number of Proscribed[[1]](#footnote-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 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 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. At the Swansea University, 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.)

1. https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2 [↑](#footnote-ref-1)