Security Sensitive Research Activities Policy

Policy Category:	General
Subject:	The management of security sensitive research activities
Approving Authority:	Academic Board
Responsible Officer:	Senior Vice President (Operations)
Responsible Office:	Research Governance Ethics and Integrity
Related Procedures:	Security Sensitive Research Activities Procedures
Related College Policies:	IT Acceptable Use Policy Information Security Policy Procedure for Investigating and Resolving Allegations of Research Misconduct Health, Safety and Welfare Policy Safeguarding Policy International Regulations Policy and Guidance
Effective Date:	June 2023
Supersedes:	N/A
Next Review:	June 2026

---

1. Purpose & Scope

1.1 King's College London supports the academic freedom of its researchers to conduct scholarly research activities in connection with their affiliation to the College. The University expects its staff and students to act with the highest integrity at all times, and to conduct their business in an honest and open manner, and in line with all relevant legislation.

1.2 Researchers who access security sensitive research material for the purpose of their academic research or as part of educational activities can be subject to surveillance by, and lead to, enquiries from the police or other law enforcement agencies.

1.3 If staff, students and affiliates manage their activities appropriately, they can usually proceed with these activities as normal while at the same time upholding obligations to the university, meeting regulatory requirements, and protecting the integrity and reputation of the University and its members.

1.4 This policy is designed to ensure that those who have legitimate reasons to work with security sensitive research material are appropriately protected and are not in infringement of the law. The University seeks to ensure that the freedom to pursue academic research is upheld, balanced with the need to protect our researchers from radicalisation, and to ensure compliance with relevant legislation.

1.5 This policy aims to ensure compliance with the *Counter-Terrorism and Security Act (2015)* and to enable the University to fulfil its duty to *have due regard to the need to prevent people from being drawn into terrorism,* and extremism, and to facilitate scholarly research into security-sensitive topics. Conducting research in line with this policy allows the College to assist the appropriate authorities by demonstrating that any security-sensitive material has been accessed as part of legitimate research activities.

1.6 Carrying out security-sensitive research may trigger a level of personal risk to the researcher that cannot be mitigated by the College. Whilst compliance with this policy 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 College can aim to support the researcher to the best of its ability.

1.7 This policy:

- outlines the actions the University expects its researchers to take in terms of appropriately disclosing the conduct research into security sensitive topics, and how to appropriately handle and store such material.
- assists with the identification of security sensitive topics.
- supports the mitigation and resolution of any associated risks in order to protect the researcher.

1.8 Any breach of this policy will be referred directly for investigation under the *Procedure for investigating and resolving allegations of research misconduct*, in the case of staff members and research degree students, or under the *Misconduct Regulation* (G27) of the College's *Academic Regulations* in the case of students who were not studying towards a research degree on the date of breach.

1.8 This policy applies to all King's College London employees, honorary and emeritus staff. It also applies to those students, volunteers or other members of the University community who may be involved in research, in the name of King's College London, in any capacity. This includes research undertaken for educational purposes by undergraduates or taught postgraduates as part of a taught course module.

1.9 The policy relates to all research involving security-sensitive topics conducted in the name of King's College London.

1.10 The policy complements the International Regulations Policy and Guidance which must be considered in parallel to this policy where relevant.

2. Definitions

2.1 Under this policy, and its connected procedure, "researcher" refers to any person officially connected with King's, including employees, emeritus, honorary or visiting post holders, students, contractors and volunteers.

2.2 "Students" means any individual enrolled on a course of study at the university, including undergraduate, taught postgraduate, research postgraduate or those on short courses.

2.3 Research activities considered to be "Security-Sensitive" include, but are not limited to, the access or generation of:

(i) material (including Online Material in the public domain and Digital Material) relating to terrorism, extremism, radicalisation and/or material which may be considered to contain "vocal and active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs" (*Counter Terrorism and Security Act (2015)*).

(ii) material relating to a terrorist group or proscribed organisation.

(iii) material relating to criminal, or otherwise illegal, activity.

(iv) materials which require security clearance.

(v) materials used for research commissioned by defence or security sectors.

(vi) materials that can only be obtained by accessing the 'dark web' through a specialised browser, and

(vii) materials that are illegal, related to criminal activity, or are otherwise sensitive or obscene.

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

2.5 "Terrorism" is the use or threat of action which:

(i) involves serious damage to property,

(ii) endangers a person's life, other than that of the person committing the action,

(iii) creates a serious risk to the health or safety of the public or a section of the public, or

(iv) is designed seriously to interfere with or seriously to disrupt an electronic system,

where the use or threat is designed to influence the government or to intimidate the public, or a section of the public, and the use or threat is made for the purpose of advancing a political, religious or ideological cause.

2.6 "Proscribed Organisations" are defined as terrorist groups or organisations banned under UK law, in accordance with legislative proscription criteria, by the UK Home Office. A list of which can be found here: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

2.7 The "Dark Web" refers to websites that exist behind multiple layers of encryption that cannot be accessed by using traditional search engines or visited by using traditional web browsers.

2.8 "Digital Material" refers to information, including text, images, audio and video, that is stored in digital form and is made accessible using digital technology, other than through the internet.

2.9 "Online Material" refers to information, including text, images, audio and video, that is accessible or is made available by connection to a central processor or computer network using the internet.

3. Policy

3.1 Research into security sensitive topics can put a researcher at risk of becoming:

(i) the subject of surveillance or investigation by relevant authorities.

(ii) radicalised by the material which they are accessing and handling.

3.2 The University requires all research involving security sensitive topics to be subject to the necessary registrations, approvals and permissions prior to the research commencing. At a minimum this will include the registration of the research with the *Research Governance Office* and the provision of an appropriate repository from KCL *IT Assurance* for purposes of securely storing material, but it may also include the appropriate ethical clearance where this is relevant.

3.3 In cases where the risk of the research is deemed to be high to either the researcher or the University or if the *Research Governance Office* does not have the expertise to determine if a risk has been appropriately mitigated, the registration may be deferred in confidence for expert review and authorisation by the *Security Sensitive Research Expert Advisory Panel (SSREAP).*

3.4 The University will provide a process by which researchers can register such research and receive instruction on the most appropriate storage repository. However, it remains the responsibility of all researchers to:

a) ensure that their registration remains up to date at all times by submitting a revised registration should any amendments be made to the project.

b) ensure that they use only the storage repository advised by IT for the material related to the registered project.

c) seek guidance either from their Line Manager or the *Research Governance Office* if there is any doubt as to whether their research falls under this policy.

d) ensure that all access to and storage of security sensitive research material is handled on the university network or university owned computers. The University advises against the use of personal devices, with the exception of instances where appropriate risk mitigations can be put in place as agreed through the process of registration.

e) ensure that any potential risks to the researcher, other individuals and the University are considered and appropriately mitigated.

3.5 Failure to adhere to points 3.4 a) & b) above may constitute research misconduct and may be referred to the appropriate university misconduct process for action.

3.6 It is recognised that there may be some occasions where classified data is being handled and in order to meet the government/security handling requirements, full registration will not be possible or appropriate. In such instances the research must be discussed directly with the *Research Governance Office* who will advise on the appropriate steps to be taken.

3.7 The *Research Governance Office* is responsible for reviewing registration submissions, and any updates, to make a record of activities planned to be carried out. This will ensure that should the activity be brought into question by the authorities there will be evidence for it to be established that the activity has been for the purposes of legitimate academic research.

3.8 The *IT Assurance* team is responsible for assessing the nature of the material to be accessed and determining and making available, the most appropriate and secure storage repository for the management of the data. This will take into consideration any requirements of relevant funding bodies.

3.9 If a researcher is found to have accessed material beyond what they have registered, and it is deemed to go beyond what is legitimate to have been accessed for the purposes of the academic research, or if they deliberately conceal or attempt to conceal security sensitive research activities, it will be considered research misconduct and referred immediately to the appropriate university disciplinary process for action. There may also be grounds for the University to report this to the relevant authorities.

3.10 There will be no time limitations on referral for disciplinary action as described in this policy.

4. Reporting and review

4.1 An annual report will be provided to the Senior Vice President (Operations) and a summary provided in the annual report of the Deputy College Secretary & Chief Compliance Officer to the *Audit, Risk and Compliance Committee*.

4.2 Failure to appropriately register and conduct security sensitive research may lead to investigation under the College's *Procedure for Investigating and Resolving Allegations of Research Misconduct* and as such there may be a requirement to report this to any associated funding body.

4.3 This policy and its associated procedure will be reviewed at least every three years.