Procedure for Registering Security Sensitive Research Activities

Policy Category:	General
Subject:	The management of security sensitive research activities
Related polices & procedures:	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 These Procedures are in accordance with the *Security Sensitive Research Activities Policy* and should be considered in conjunction with any instructions for using any tools provided by the University for the registration of such research.

1.2 The procedures are intended to help the University balance the freedom to pursue academic research, with the need to protect our researchers and students from being drawn into terrorism and extremism and to ensure compliance with relevant legislation. They are also intended to support the university in conducting its research in a legal, ethical and transparent manner.

1.3 The primary purpose of the procedures is to ensure that researchers and students are adequately supported in registering security sensitive research to the University in such a way that:

(i) should they ever be subject to surveillance or investigation by any authorities it can be evidenced that the security sensitive material was accessed for legitimate academic research purposes.

(ii) the University has sufficient oversight of the research being undertaken to ensure that researchers are not at risk of becoming radicalised.

1.4 The secondary purpose of the procedures is to provide staff and students with a framework within which they can design a management plan for handling security sensitive material.

1.5 These procedures apply 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.

1.6 The procedures relate to all research involving security-sensitive topics conducted in the name of King's College London. This includes research undertaken for educational purposes by undergraduates or taught postgraduates as part of a taught course module.

2. Definitions

2.1 Definitions are contained in the *Security Sensitive Research Activities Policy*.

3. Procedures

A. Procedures for identifying security sensitive research

3.1 In advance of any collection of research materials, the researcher must identify whether their project constitutes security-sensitive research and therefore is covered under this Policy. They can do so by having clearly defined the research methods they intend to use to conduct their research and the type of research material they intend to analyse. Section 1 of the *Security Sensitive Research Registration Form* can also be used as a checklist to determine if this policy applies.

3.2 Students should discuss their research with, and obtain approval from, their supervisor, before registering their project under this policy.

3.3 If there is any doubt as to whether a research project falls under this policy, researchers should discuss with their supervisor or Line Manager as appropriate or with the *Research Governance Office*.

3.4 Although onus is on individual researchers to appropriately register security sensitive research, supervisors and line managers should make reasonable efforts to be broadly aware of the nature of the research their staff or students are conducting and direct them to these procedures as appropriate.

3.5 It is recommended that researchers discuss security sensitive research with their supervisor or Line Manager at as early a stage as possible, in order that any special provisions that might need to be made for the research in terms of facilities or resources can be considered and feasibility determined.

B. Procedures for registering security sensitive research

3.6 The University requires all researchers who have determined that they are conducting security sensitive research to register this with the *Research Governance Office*.

3.7 The registration procedure is not a substitute for ethical clearance from the College's Research Ethics Committee and researchers must consult Research Ethics Office webpages to ascertain whether their project requires ethical clearance ahead of any data collection. In instances where research ethics review is determined to be required, the project must also be registered with the Research Governance Office.

3.8 The registration process is not a substitute for any requirements to be followed under the International Regulations Policy and Guidance and researchers must consult this policy to ascertain whether their project requires any other approvals or licence applications before the research can commence.

3.9 Researchers must register their research by completing the Security Sensitive Research Registration Form, which must include the details of the material to be collected and also a risk assessment of the research. Proper consideration must be given in completing the risk assessment to other University Policies and Procedures that may be relevant such as IT and health and safety.

3.10 If students will be accessing any security sensitive research material as part of an activity which falls within the learning aims and objectives of a taught module, the Security Sensitive Research Registration form for Taught Modules should be completed by the module leader and submitted to the *Research Governance Office* for registration prior to commencement of the activity.

3.11 If, as part of a Taught Course Module, students will be conducting individual research projects in which the activity does not fall within the learning aims and objectives of the course but is instead a stand-alone research project for which each student has their own specific aims and objectives, then an individual Security Sensitive Research Registration form must be submitted by each student.

3.12 The security sensitive research registration forms will be securely stored on the university network and will be managed by the *Research Governance Office*. However, where circumstances require it, they may need to be accessed by:

(i) University management, including faculty and directorate line management or staff in Research Management and Innovation Directorate or IT who are responsible for collaboratively overseeing the system of support for security sensitive research.
(ii) Internal Auditors or any university manager who has been requested to investigate any allegations relating to the conduct of security sensitive research.
(iii) External auditors, including assurance staff from external funding bodies.
(iv) The relevant authorities.

3.13 The completed form must be submitted to the *Research Governance Office* as per the details given on the registration form. The form will be reviewed by the *Research Governance Office* to ensure that the researcher has identified any risks and that these have been mitigated with appropriate safeguards.

3.14 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) before confirmation to commence can be granted.

3.15 The researcher will complete the high-risk checklist as part of the *Security Sensitive Research Registration Form* and as such will be aware upon submission if the research has been deemed high risk and will require SSREAP review. The *Research Governance Office* will determine the nature of expertise required on a case-by-case basis and the appropriate members of SSREAP will undertake a high-risk review. In exceptional cases the SSREAP may convene as a full panel where the risks of the research are not limited to a specific area of expertise.

3.16 If a project is escalated for high-risk review and the SSREAP determines that the research is too high-risk to proceed in its current form, they will provide feedback to the *Research Governance Office*, who will relay this feedback to the researcher, with any changes that could be made to enable the research to proceed. The onus is then on the researcher to consider and make these changes if they wish to proceed. Where appropriate changes cannot be made in order to mitigate elements of the project identified as high risk, registration will be declined, and the research cannot commence.

3.17 In cases where it has been determined that the registration can be confirmed, the researcher will be issued with a confirmation email outlining the registration.

3.18 The *Research Governance Office* email will be copied to the *IT Assurance* team who the researcher will then be required to liaise with in order to determine the appropriate IT facilities to be used for the access, management and storage of the security sensitive material.

3.19 Security sensitive research can only commence after both *Research Governance Office* confirmation has been received and the appropriate IT support/solution has been provided.

C. Procedure for handling security sensitive material

Access

3.20 When accessing web sites or otherwise accessing online content that might be associated with illegal activities, radicalisation or terrorist/extremist organisations or groups, researchers should be aware that such activity may be subject to surveillance by the police or other law- enforcement agencies and that visiting such sites or otherwise accessing online content that could be interpreted as promoting and/or endorsing radicalisation, terrorism or extremism can put them at risk of enquiries by the authorities.

3.21 Should researchers need to visit such sites or otherwise access online content when undertaking legitimate research, they should do so from the University network (including the wireless network and VPN) and from computers which are University-owned and used primarily for university business. Accessing these materials from a university network will help to demonstrate that these activities are part of legitimate research.

3.22 The University recognises that it may not always be practical to use the University network or University computers when accessing sensitive material for research purposes. In such cases the use of non-University IT equipment may be permissible, providing appropriate risk mitigation safeguards have been identified in a researcher's *Security Sensitive Research Registration* and those safeguards been agreed by the *Research Governance Office* in consultation with IT Assurance where appropriate.

3.23 If a researcher does not have access to a University-owned computer and the risks posed by the research are deemed too high for the use a personal device, researchers may be able to loan a device from their department for the duration of the project. Alternatively, grant funded researchers should consider costing a dedicated device into the budget of their grant.

Storage

3.24 All security sensitive material must be stored in a solution with restricted access that has been approved for use by IT. The preferred and supported solutions are a KCL SharePoint Online site and/or OneDrive for Business. The choice of which to use will be determined by the nature and access requirements to the data. Confirmation as to which of these solutions is appropriate for any given research project must be agreed by *IT Assurance* and any exceptions to the usage of these options will be at the discretion of *IT Assurance* or will require justification from the researcher and should be clearly stated in the SRR application.

3.25 It is important to note that due to the contract KCL have with Microsoft and the terms and conditions; if owning, viewing or storing the research material would constitute a criminal act or breach of regulations, then this should be raised and discussed prior to conducting the research.

3.26 For storage related queries, researchers are advised to raise a ticket via the *IT Service Desk* and it will get directed to *IT Assurance*. In the short description for the ticket, researchers should state: 'FAO IT Assurance: Data Storage advice required – security sensitive research'.

3.27 Researchers must limit the access to security-sensitive materials to their supervisor or named collaborators identified on the *Security-Sensitive Research Registration Form*. In instances where the material does need to be transferred or shared outside of the agreed storage solution, the mechanisms for sharing and risk mitigations must be addressed in the risk assessment.

D. Procedure for handling issues raised

3.28 Any enquiries from the police or other recognised authorities will be directed to the University's Head of Security. The *Research Governance Office* and the *IT Assurance* team will then liaise with the Head of Security to consider any requests for access, to determine if access will be permitted and to chaperone access if it is granted.

3.29 If any staff or students become aware of any colleagues engaging in security sensitive activities, or if materials related to terrorism or extremism are discovered on campus, this must be reported to the Head of Security in the first instance. The Head of Security will then liaise with the *Research Governance Office* to check if the activity is registered for research purposes and if not, will be obligated to take appropriate action.

3.30 Any breaches of the policy and procedures will be considered under the University's *Procedure for Investigating and Resolving Research Misconduct*.