Security Sensitive Research

City supports the principle of academic freedom and aims to support the scholarly research activities conducted under its auspices. This includes research into security sensitive areas such as:

- accessing websites relating to terrorism, radicalisation and/or downloading material considered ‘extremist’ (this is defined as, ‘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’ in the Counter Terrorism and Security Act (2015));
- primary criminal or illegal activity;
- materials which require security clearance;
- materials used for research commissioned by the military or under an EU security call; and
- research into prohibited organisations.

Please note that this list is not exhaustive. For further advice, please contact the Research Governance & Compliance Manager in Research & Enterprise.

In order to facilitate research into such topics, but to protect staff and students, a registration process for research projects into these areas has been put in place. The registration process is a mechanism that enables City to demonstrate the legitimacy of the research, should this prove necessary, and is not put in place to regulate such research.

Researcher need to be aware that there is a degree of personal risk in undertaking this research and that City cannot guarantee protection from investigation or criminal prosecution by external authorities even if the project is registered.

The registration process applies to all research projects undertaken by students and staff (including UG and PG) involving access, collection and use of security sensitive materials, and applies to all research being undertaken under the auspices of City. Research project(s) must be registered before the research can commence. Breach of this policy will be investigated through the normal institutional misconduct procedures.

City has a responsibility to seek to ensure that its staff and students are not adversely affected by the research being undertaken. This needs to be considered before the project commences, with a prior risk assessment being undertaken. Where students are undertaking research that may be distressing, it is the supervisor’s responsibility to ensure that the student is supported appropriately. This can be achieved by, for instance, additional supervisory meetings.

Registration process
Research that falls within the definition of security sensitive research has to be registered using the Registration Form and submitted to the Research Governance & Compliance Manager, Research & Enterprise. The registration form must be signed off by the supervisors in the case of student research, and the Head of Department or Associate Dean for Research in the case of members of staff. This will demonstrate to Research & Enterprise that the Department/School is aware of the research being undertaken.
Research Shared Drive
Once the project has been registered with Research & Enterprise, a research shared drive for storing the security sensitive material will have to be set up. The researcher will need to make a request in Service Now to arrange for the drive. This request will be allocated to the IT Business Relationship Manager who will discuss the request with the researcher to ensure all the requirements of the project are captured and able to be met. Upon approval a standard, password protected shared drive will be created for the researcher and their collaborators. In the event a higher level of data sensitivity of data is required and the data must be held encrypted, Information Technology would need to understand further detail on the specific encryption requirements and the processes by which the data would be accessed to procure a necessary solution.

Storing material
Any security sensitive research material must be stored on the institutional password protected research shared drive. Note that material must not be stored on the researcher’s personal computer, on a City computer or on a standard institutional drive. A password protected project drive will be allocated once the project has been registered and approved.

Physical outputs (e.g. reports, manuals, CDs) must be scanned and a copy uploaded to the secure project drive. Hard copies should be destroyed securely once the scanned copy has been saved to the drive.

Documents stored on the project drive will only be accessible to the researcher and must only be shared with named collaborators. The Research Governance & Compliance Manager will be notified of the names of the files on the drive when they are uploaded and will have access to the metadata. This will enable the institution to have oversight of the material and allow for prompt responses should any internal or external enquiries relating to the use of security sensitive material be received.

Accessing security sensitive websites
All staff and students should be familiar with City’s Acceptable Use of Telephones, Email and Internet policy and Conditions of Use and in particular the sections dealing with access to offensive and security sensitive information.

Security sensitive research involving human participants
All research projects involving human participants and/or personal data are subject to review by one of City’s Research Ethics Committees. Security sensitive research projects involving human participants and/or personal data must be submitted to Senate Research Ethics Committee for review. For further advice, please contact the Research Governance & Compliance Manager in Research & Enterprise.

External Enquiries
Enquiries from legitimate external bodies or members of staff or students at City should be directed to the Research Governance & Compliance Manager.

Further Guidance
Materials covered by the Official Secrets Act (1989)
Materials covered by the Terrorism Act (2006)
Prevent Duty Guidance for higher education institutions in England and Wales
Universities UK, Oversight of security-sensitive research material in UK universities: guidance

This policy will be reviewed and updated as required.