Policy and Process for Managing Security-Sensitive Research (SSR)

1. Introduction and purpose

The UK Counter-Terrorism and Security Act 2015 imposes a duty on Universities to 'have due regard to the need to prevent people from being drawn into terrorism'. This requires the University to have policies and processes in place for all staff or students working on sensitive or extremism-related research (including learning and teaching activities that include an element of research or academic enquiry). This document sets out the University of Sheffield's requirements for the use of such materials in research, and seeks to balance academic freedom with the need to have proportionate processes and safeguards in place.

The primary aims of this policy are therefore to:

- Ensure the welfare of staff and, in particular, students who undertake security-sensitive research, recognising the *potentially* radicalising and/or distressing effects of viewing security-sensitive material;
- Protect staff and students undertaking legitimate research from misinterpretation by the authorities (which may result in legal sanction), so that research may proceed unhindered.

This Policy forms part of a suite of resources provided by the University to meet its obligations under the UK Counter-Terrorism and Security Act. Further information can be found on the Research Services website:
https://www.sheffield.ac.uk/rs/ethicsandintegrity/security-sensitive-research

Related information and guidance about preventing radicalisation can be found on the Student Support Services website:
https://www.sheffield.ac.uk/sss/safeguarding-overview/prevent

2. Scope of this policy

This policy applies to research that relates to groups that are on the Home Office list of 'Proscribed terrorist groups or organisations'. The list is available at the following web address:
https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

It should be noted that the list may change during a project's lifetime, and hence staff who are involved in (or who supervise students who are involved in) areas of research that are most likely to come within the scope of this policy should keep the list under regular review. Should an on-going project become within the scope, the process set out below should be followed.

Other potentially high-risk areas of research (e.g. research into paedophilia, animal rights campaigning, or Ministry of Defence-commissioned work on military equipment) are outside the scope of the policy. Issues relating to such research should be considered, in the first instance, at a department level (e.g. as part of standard departmental processes such as student supervision and monitoring, academic/ethical review, risk assessment); issues may be referred to Security Services if deemed appropriate.

3. Process for managing security-sensitive research

The University has defined three categorises of risk relating to SSR; the categories, and the processes that should be followed in relation to each, are set out below.

Level 1 (lower security risk) research: Research that is related to aspects of the activity of Proscribed Terrorist Groups or Organisations, but which does not specifically require direct access to the materials of the Proscribed Groups, or contact with the Groups themselves

(either online or otherwise) (e.g. groups of students asked to look at news reports relating to terrorist activity for a research assignment).

Process: Departments, module coordinators and supervisors should be aware of the *potential* risks of asking students to undertake this kind of work and should ensure that, where relevant, processes are in place to ensure that such concerns are discussed with students. The University anticipates two main potential risks, as follows (although others may arise):

1. A low risk exercise escalating into a higher risk category (e.g. where a student goes beyond the intended scope of the exercise by following a series of links, resulting in them accessing material from a proscribed group).
2. Students working on activities that may potentially have a negative impact on others around them when working on PCs in common study areas and public spaces.

Staff may need to discuss with students the importance of taking a common sense approach and setting appropriate boundaries; departments/members of staff may also seek advice from the Information Security Manager in Corporate Information and Computing Services (CiCS) with regard to how to manage these issues.

Level 2 (medium security risk) research: Research that involves accessing/downloading information that is linked to groups on the Home Office list of 'Proscribed terrorist groups or organisations', but where there is no intention for direct contact/interaction with group members to take place.

Process: No referral to Security Services is required; however, the following steps should be taken:

(1) advice should be sought in the first instance from the Information Security Manager in Corporate Information and Computing Services (CiCS), who will, wherever possible, support the researcher and their department in putting an appropriate framework in place for managing the research;

(2) the relevant department should undertake a detailed risk assessment (to be signed off by the Head of department), and a record of this should be kept. This would need to be presented on request should an individual come to the attention of any prosecution agency where the University may need to show that due process has been followed.

Level 3 (high security risk) research: Research that involves direct contact/interaction with groups on the Home Office list of 'Proscribed terrorist groups or organisations' (e.g. actively joining social media groups, engaging in discussions (online or otherwise). [It should be noted that it is a criminal offence to 'belong, or profess to belong, to a proscribed organisation in the UK or overseas', along with a number of other actions relating to involvement with a proscribed group. The University would be unable to support a researcher engaging in illegal activity. The full list of criminal offences associated with proscribed groups can be found here: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2].

Process: The lead researcher (in the case of a student, this would be the supervisor) should refer the situation to their Head of Department, who should then contact the Head of Security (or a relevant deputy) **as early in the project planning stage as possible**, providing details of the proposed project. The Head of Security will work with the Head of Department to undertake a detailed risk assessment and put in place a proportionate framework for managing the research, drawing on advice from other areas of the University or seeking advice from relevant external agencies where appropriate. It should be noted that it may be necessary in some cases for the Head of Security to divulge the name of the researcher to the authorities in order to ensure that they are afforded sufficient protection from legal sanction.

*Queries about this Policy and Process can be directed to Lindsay Unwin in Research Services (l.v.unwin@sheffield.ac.uk, x21443) in the first instance.