### Draft Flowchart for Process of Managing Security-Sensitive Research (SSR)

**Step 1:** Does your research relate to groups that are on the Home Office list of ‘Proscribed terrorist groups or organisations’?  
[https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations-2](https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations-2)

**If yes, move to Step 2**  
If no, no further action required

**Step 2:** Identify the category of risk that applies to your research and follow the appropriate process:

<table>
<thead>
<tr>
<th>Level 3 (high security risk) research</th>
<th>Level 2 (medium security risk) research</th>
<th>Level 1 (lower security risk) research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEFINITION:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research that involves <strong>direct contact/interaction</strong> 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))</td>
<td>Research that involves <strong>accessing/downloading information</strong> 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.</td>
<td>Research that is related to aspects of the activity of Proscribed Terrorist Groups or Organisations, but which involves <strong>no direct contact with, or access to the materials</strong> of Proscribed Groups (e.g. groups of students asked to look at news reports relating to terrorist activity for a research assignment).</td>
</tr>
<tr>
<td><strong>PROCESS:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The lead researcher (in the case of a student, this would be the supervisor) should:</td>
<td>No referral to Security Services is required. However, the lead researcher should:</td>
<td>The lead researcher / module coordinator / supervisor should:</td>
</tr>
<tr>
<td>(1) Refer the situation to their Head of Department, who should then contact the Head of Security (or a relevant deputy) <strong>as early in the project planning stage as possible</strong>, providing details of the</td>
<td>(1) Seek advice from the Information Security Manager in Corporate Information and Computing Services (CiCS) [Chris Willis: <a href="mailto:c.willis@sheffield.ac.uk">c.willis@sheffield.ac.uk</a>, ext. 23127]:</td>
<td>(1) <strong>Be aware of the potential risks</strong> of undertaking / asking students to undertake this kind of work. [The University anticipates two main potential risks, as follows (although others may arise):</td>
</tr>
</tbody>
</table>
| Proposed project | The Head of Security will work with the Head of Department to undertake a detailed risk assessment and a record of this should be kept. | Ensure that a detailed risk assessment is undertaken according to the relevant departmental process (to be signed off by the Head of department), and a record of this should be kept. | 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. |

| 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. | Discuss the risks with those involved as appropriate, according to their level of experience. In particular, staff may need to discuss with students the importance of taking a common sense approach and setting appropriate boundaries. |

*Departments/members of staff may seek advice from the Information Security Manager in Corporate Information and Computing Services (CiCS) if required [Chris Willis: c.willis@sheffield.ac.uk, ext. 23127].

**WHAT HAPPENS NEXT?**
The Head of Security will advise the Head of Department, and work with them to put in place a proportionate framework for managing the research.

This may involve drawing on advice and support from other areas of the University (e.g. CiCS) and/or seeking advice from relevant external agencies where appropriate (e.g. the North of England Counter-Terrorism Unit).

Safeguards may include:

- Informing relevant external agency/ies of the proposed research project [it may be necessary for the Head of Security to divulge the name of the researcher(s), in seeking to afford them sufficient protection from potential legal sanction]
- Provision for researchers to access material in a private room and/or using a designated computer;
- Monitoring by CiCS of the material being viewed online from a designated PC;
- For students, appropriate levels of supervision may be required whilst undertaking research activities (in such cases, supervisors should look out for signs that students are uncomfortable with, or distressed by, the activity and should take appropriate steps (e.g. offering to discuss the situation with the student, suggesting the student takes a break from the work, signposting the student to appropriate support such as the SSiD Health and Wellbeing webpages.

Departments should maintain records of the risk assessments undertaken for relevant research projects, as these 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.

CiCS will advise, and where possible, support the lead researcher and their department with respect to putting in place a proportionate IT framework for managing the research.

Safeguards may include:

- Provision for researchers to access material in a private room and/or using a designated computer;
- Monitoring by CiCS of the material being viewed online from a designated PC;
- For students, appropriate levels of supervision may be required whilst undertaking research activities (in such cases, supervisors should look out for signs that students are uncomfortable with, or distressed by, the activity and should take appropriate steps (e.g. offering to discuss the situation with the student, suggesting the student takes a break from the work, signposting the student to appropriate support such as the SSiD Health and Wellbeing webpages.
student to appropriate support such as the SSID Health and Wellbeing webpages. Further advice for staff on student wellbeing can be obtained from the Central Welfare and Guidance Team):

- Holding discussions with relevant researchers/students and their supervisors, to ensure that they are aware of the potential risks and how to manage them.

*For further advice on this process and when it applies, you can contact Lindsay Unwin, Research Services (x21443; l.v.unwin@sheffield.ac.uk)

*This flowchart 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