Guidance for Staff on Managing Security-Sensitive Research (SSR)

What is Security-Sensitive Research?

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, regardless of the level of skill or experience of the researcher. Security-Sensitive Research is defined as research involving 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

What Policy and Process does the University have in place?

The University has in place a **Policy and Process for Managing Security-Sensitive Research** (including learning and teaching activities which involve an element of research or academic enquiry) which seeks 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).

The Policy and Process can be found here:
https://www.sheffield.ac.uk/rs/ethicsandintegrity/security-sensitive-research

How does this apply to me?

- **All University staff who undertake or support research, and/or are in a student-facing role** should be aware of the Policy and Process so that they can direct colleagues or students to the appropriate resources should the need arise.

- **Staff members who undertake research that may fall under the remit of the Policy, or who run modules for/supervise students who may undertake research that falls under the remit**, should familiarise themselves with the Policy, follow the Process as required, and take both into consideration in the planning of relevant projects, modules and as part of supervision discussions. [If any member of staff is unsure whether the Policy applies to their research or that of their student(s) they can contact Lindsay Unwin in Research Services (l.v.unwin@sheffield.ac.uk, x21443) in the first instance.]

I will be doing/some of my students will be doing projects that may fall into the category of Security Sensitive Research – what key issues should I be aware of?

It is important to consider carefully the risks of undertaking SSR, and to have open discussions with relevant research colleagues / students according to their level of experience, incorporating the requirements of the Policy and Process. You may want to raise:

- The importance of taking a common sense approach and setting appropriate boundaries to avoid a low risk exercise escalating into a higher risk category (e.g. being careful of following links on websites into the so-called 'dark web' where access to sites may be monitored by the authorities; avoiding unnecessarily downloading everything that can be found on the internet that relates to a particular topic/group, as this may attract attention from the authorities).

- The need to have an awareness of the potential impact of research activities on those around, such as when working on PCs in common study areas or public spaces, where others may see materials being viewed and either be offended or concerned about the person's intentions.
- The need to have an awareness of the potential impact of research activities on the researcher's own well-being and mind-set, particularly if viewing very distressing material, and to seek support and advice from an appropriate source (e.g. supervisor, module leader, the University's Mental Wellbeing resources or Counselling Service).
- Security sensitive websites MUST NOT be accessed from personal computers. CiCS can provide advice on IT arrangements and provide IT equipment for security sensitive research where appropriate.
- Extra care should be taken when storing data and materials related to security sensitive research. Hard copies of security sensitive research material should be stored in a secure location, or uploaded to an appropriate secure filestore and the hard copy destroyed.

*This guidance 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