

## Sensitive Research Policy and Procedure

<b>Fersiwn: Version:</b>	<b>Dyddiad: Date:</b>	<b>Cymeradwywyd gan: Approved by:</b>	<b>Dyddiad adolygiad: Review Date</b>
Final	February 2017	UREC   Executive   Prevent Group	February 2018

## Contents

1. Introduction.....	2
2. Sensitive Research.....	2
3. Undergraduate and Taught Postgraduate Students .....	3
4. Approval and Access Process .....	3
5. Accessing Prohibited Sites .....	4
6. Storing Material.....	5
7. Transmitting Material .....	5
8. Internal and External Queries .....	6
9. Non-adherence to policy.....	7
10. Policy review.....	7

### 1. Introduction

1.1 The University acknowledges that academic freedom is key in relation to its research activities. However, the University also has a duty to ensure that research, particularly research that is sensitive in nature, is conducted ethically and appropriately.

1.2 Naturally, research into sensitive areas carries a degree of risk for the researcher conducting it. Compliance with this policy note allows the University to demonstrate to external authorities that any such material forms part of legitimate research. However, the University cannot guarantee that this will provide protection from investigation by such authorities, should the situation ever arise.

1.3 The scope of this policy applies to all those, including staff and students, conducting research for and on behalf of the University.

### 2. Sensitive Research

2.1 There are three broad research areas which would usually cause the research to be classified as 'sensitive':

- i. **Research into illegal activities;** although please see the separate guidance on this.
- ii. **Research which requires access to web sites which would normally breach [Information Services Regulations](#),** including, but not limited to; pornography, or the sites of any of the [organisations](#) proscribed by the UK Government;
- iii. **Research into extremism and radicalisation.**

2.2 The definition of sensitive research encompasses a wide variety of research topics, and it is a requirement to complete the relevant questions in the *online ethics assessment form*, in order to ascertain if a research project is likely to be considered sensitive research in accordance with this policy.

2.3 It is further acknowledged that every research project is unique in its aims and methodology. Therefore the researcher and supervisory staff should ensure that they consider the ethical dimensions of the proposed project in a proactive and candid manner, in accordance with the aims of this policy.

### **3. Undergraduate and Taught Postgraduate Students**

3.1 It is not appropriate for undergraduate students to undertake any sensitive research due to their relative inexperience with research, unless specific circumstances of oversight and evaluation have prevailed. Supervisors and module co-ordinators will need to give careful consideration to the potential for some sensitive research areas to cause harm to the mental health and wellbeing of students.

3.2 It is only appropriate for taught postgraduate students to undertake any of the research activities listed in 2.1 with due oversight and evaluation by the supervisory team and Head of Department.

### **4. Approval and Access Process**

- 4.1. The online ethics assessment form contains a sensitive research appendix with a series of filter questions. These identify if a research project should be classified as sensitive, and as such requires special consideration before ethical approval can be granted.
- 4.2. The appropriate departmental or institute based reviewer, along with the Research Ethics Unit will make a collective decision whether or not to grant sensitive research projects departmental ethical approval. The Chair and at least two other members of the relevant University Research Ethics Panel (including an independent member and student representative, if the researcher is a student) will discuss the application and decide whether to allow the proposal to remain within the department, or to request changes to the research design/protocol through the submission of an application to the relevant Research Ethics Panel.
- 4.3. A decision on whether ethical approval will be given to the applicant, including any changes that may be required, will be made by Department/Institute and Research Ethics Unit within 10 days of the submission of the online assessment. If the researcher is required to submit an application for formal REP review, the application will be considered at the next Panel meeting date.
- 4.4. Applicants who are refused ethical approval with no option to amend their research design/protocol (something which should be very rare) may appeal in writing, following the procedure as outlined on the Research Ethics web page.
- 4.5. Any deviation from the methods surrounding security sensitive research that has been granted full ethical approval is not permitted. If the research requires any change, such as accessing new materials, or undertaking new areas of investigation, then a resubmission for ethical approval will need to be made. Every effort will be made by the Research Ethics Panels to process this new application as quickly as possible so as not to

delay the research.

- 4.6. Once ethical approval has been granted to a research project classified as sensitive, the Research Ethics Unit will issue confirmation to Information Services and will request that a secure password-protected separate file store be made available to the researcher. The file store must then be used as the sole storage method of any material considered as sensitive and material should not be accessed before the researcher has been granted access to the file store.
- 4.7. Once ethical approval has been granted, the project details will be recorded on a register by the Research Ethics Unit. An up-to-date copy of the register will then be shared with the Director of Information Services, the Director of Research, Business & Innovation and the Pro Vice Chancellor, Chief Operating Officer in the event of any external queries.
- 4.8. An End of Project report is required to be submitted to the Research Ethics Panel that granted the final ethical opinion. This will be provided to the researcher once approval has been granted. It is the responsibility of the researcher to ensure that this is returned within one month of the project end date.
- 4.9. UREC will oversee the implementation of this policy and the approval process.

## 5. **Accessing Prohibited Sites**

- 5.1 Researchers whose projects have received full ethical approval and who require access to web sites which may breach the [University Information Services Regulations](#) must contact the Research Ethics Unit to ensure that Information Services can make the necessary permission changes and record the identity of the individual/s requiring access.
- 5.2 Researchers who access web sites that might be associated with radicalisation or terrorist/extremist organisations or groups should be conscious that such sites may be subject to surveillance by the police, and that accessing those sites might lead to police enquiries. Once full ethical approval has been granted, researchers should use the University network to access such sites. This will ensure these activities are flagged as a legitimate part of their research. However, as stated, the University cannot guarantee protection from investigation by external authorities.
- 5.3 Where there is any uncertainty, the researcher should not access such websites and contact the Research Ethics Unit to ensure that they have received the appropriate ethical approval and permissions from Information Services.

## 6. Storing Material

- 6.1 Certain types of sensitive research require additional considerations, including
- i. Research into terrorism, extremism, terrorist or extremist organisations or groups, extremist ideologies, radicalisation<sup>1</sup>, de-radicalisation<sup>2</sup>;
  - ii. Research commissioned by the military or GCHQ;
  - iii. Research commissioned under an EU / US security call or similar;
  - iv. Research involving the viewing, usage or transfer of sensitive personal data as defined as such by the Data Protection Act 1998;
  - v. Research involving the acquisition of security clearances (including the Official Secrets Act).
- 6.2 All research materials and data for research into the areas listed in 2.1 must be stored securely in the aforementioned password-protected separate file store. No copies should be kept in any other location. If provision for secure storage has not already been arranged as part of the project, it is the responsibility of the researcher to contact the Research Ethics Unit to request access.
- 6.3 Researchers must ensure that the University has the capacity and capability to fulfil any further obligations as laid out by the relevant research funding body or organisation.
- 6.4 Access to this file store must be restricted to the researcher, and any internal co-investigators working on collaborative projects. The secure storage arrangements must include all materials related to the research project, including but not limited to: downloads, documents, videos, images, or research data. Access to this file store can be revoked if the researcher leaves the project, or fails to comply with this policy.
- 6.5 Online sensitive research that has received ethical approval into the areas listed in 2.1 should be conducted on University servers (see 5.1).
- 6.6 Physical documents and data should be scanned and uploaded to the password-protected server; where this is not possible, documents should be kept in a locked filing cabinet, in a locked, single-user office on University premises.

## 7. Transmitting Material

- 7.1 Researchers should note that the Terrorism Act (2006) and the Counter-Terrorism and Security Act (2015) outlaw the dissemination of terrorist publications if the individual concerned has the intention to encourage or induce others. For the latter legislative provision, researchers must note that '*reckless behaviour*' may still amount to an offence under the Act. Publications disseminated for the purposes of a clearly defined research project should not amount to an offence, because the requisite intention is unlikely to be present. However, caution is advised and the dissemination of raw research materials should be avoided where possible.

---

<sup>1</sup> Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

<sup>2</sup> De-radicalisation usually refers to activity aimed at a person who supports terrorism and in some cases has engaged in terrorist related activity, which is intended to effect cognitive and/or behavioural change leading to a new outlook on terrorism and/or disengagement from it.

- 7.2 In the instance of collaborative research projects with researchers at other institutions in the UK or abroad, the sending of documents may occasionally be necessary. Documents should be individually password-protected where possible, and then sent using a secure method which encrypts the file during transmission. Co-Investigators from outside the University may also send files to researchers at AU, which must then be stored immediately in the secure file share. Information Services can provide advice on the secure transmission.
- 7.3 Researchers are strongly advised to avoid transporting raw research materials connected to sensitive research projects. However, if it is unavoidable researchers must use an encrypted memory stick.
- 7.4 Researchers should exercise caution when using personal social media to disseminate critical arguments or the outputs or outcomes of sensitive research projects for the reasons stated in 7.1. In particular, it is strongly advised that researchers do not create hyperlinks to sites used, with ethical approval, as 'raw research materials' (e.g. sites of any [proscribed organisations](#)). Additionally, researchers should adhere to the relevant [Information Compliance](#) policies.

## 8. **Disposal of Material and Data**

- 8.1 The disposal of research material (hard-copies) should be carried out by the researcher, ensuring that all material is disposed of in an appropriate manner that renders it inaccessible to others. The transporting of material long distances should be avoided.
- 8.2 Material stored electronically, on the password-protected server, will be securely erased once access to the secure drive has lapsed or when access is no longer required.
- 8.3 Where research data management requirements exist, researchers should ensure that any data, whether in digital or physical form, earmarked for disposal after the collation process at the end of the project is disposed of as in 8.1 and 8.2.
- 8.4 It is the researcher's responsibility to ensure that all other ethical, legal and procedural guidelines have been adhered to in the disposal of any such data. Including, but not limited to, AU policies, procedures and funding body guidance.

## 9. **Internal and External Queries**

- 9.1 If anyone has genuine concerns related to the use or misuse of sensitive research materials by any member(s) of staff or student(s) they should contact the Pro-Vice Chancellor (Chief Operating Officer) in non-urgent situations. If the concerns relate to the content of any hard copy materials (e.g. books or printed papers) the materials should be left untouched, but the finder should stay with them whilst a senior member of staff verifies if these materials relate to a legitimate research project. Similarly, electronic material should not be viewed until its contents can be verified by the appropriate authorities.

## 10. Non-adherence to policy

- 10.1 Breach of this policy through failure to gain ethical approval for sensitive research, deviation from the research design originally submitted for ethical approval, or failure to store research materials for research into the areas listed in 2.1 securely, forfeits any protection the University can offer should external authorities launch an investigation. Normally breaches of this policy by both staff and students will be investigated through the [Misconduct in Research policy](#)

## 11. Policy review

- 11.1 This policy will be reviewed annually by the University Research Ethics Committee.