

## **Process for researchers seeking permission to undertake security sensitive research using University ITS resources**

### **Background**

In October 2015, the University Research Governance Committee (URGC) reviewed a University statement that set out the legal requirement of the institution to release confidential research data. As an outcome of this statement, the Research Governance Officer was asked to prepare a *proforma* for completion by researchers to permit access to sensitive material in a managed manner that protected researchers and ensured that individuals with key responsibilities are aware of such activities should agencies such as the Police have queries about their legitimacy.

The following *proforma* (see below) has also been developed in response to queries from researchers working in the area of research into the online activities of extremist groups who align themselves to terrorist activities. The University recognises its statutory responsibilities to engage with the Prevent agenda as stipulated by the Counter Terrorism and Security Act of 2015.

The University also notes the Universities UK document 'Oversight of security-sensitive research material in UK universities: guidance' (October 2012) that proposes a framework for managing sensitive material in parallel with existing ethical review processes.

As part of this process, following ethical review, the researcher agrees to restrict their accessing of any sensitive materials to using specified IT resources and data storage. This serves to help protect the researcher and the institution from any unauthorised activities or subsequent dissemination of sensitive material downloaded from the internet that would be in contravention of the University's Prevent duties<sup>1</sup>.

The researcher is, however, granted sufficient access to undertake work effectively whilst ensuring that the University has sufficient means to have oversight of the activity and allow appropriate responses to queries from both external law enforcement agencies (or similar) and internal University services (such as ITS and the Office of Planning, Governance and Compliance) by awareness of ethically approved research activity.

Queries about the validity of such research and whether it has been subject to the necessary approvals should be addressed to the Research Governance Officer<sup>2</sup> in the first instance.

### **Process**

Researchers undertake the following processes sequentially

1. Application for standard ethical review by the relevant C-REC through the online application system on Sussex Direct (High Risk route)

---

<sup>1</sup> [http://www.legislation.gov.uk/ukdsi/2015/9780111133309/pdfs/ukdsiod\\_9780111133309\\_en.pdf](http://www.legislation.gov.uk/ukdsi/2015/9780111133309/pdfs/ukdsiod_9780111133309_en.pdf)

<sup>2</sup> [rgoffice@sussex.ac.uk](mailto:rgoffice@sussex.ac.uk)

2. Submission of the *Application for specific University IT resources to enable security sensitive research* form to the ITS helpdesk ([rt-its-helpdesk@sussex.ac.uk](mailto:rt-its-helpdesk@sussex.ac.uk)). The ER number generated by Sussex Direct shall be cited on the *proforma*.
3. Submission of the *proforma* (below) to the **Research Governance Officer** ([rgoffice@sussex.ac.uk](mailto:rgoffice@sussex.ac.uk)) following Head of School approval. The applicant shall cite the help desk reference number issued by ITS on the *proforma*.
4. **Review by an ad hoc review sub-committee of the University Research Governance Committee (URGC)** to review requests for access to IT facilities to conduct sensitive research<sup>3</sup>. Upon approval, a nominated contact in ITS and the Director of Governance, Planning and Compliance shall be informed. The applicant will be notified of the outcome of the review.

Approval shall be granted for specific periods of time only with extensions to the period requiring the submission of an amendment through the ethical review process and further consideration by the URGC's review sub-committee

### **IT specific conditions**

In accordance with Universities UK guidance<sup>4</sup>, it is proposed that any sensitive research activity and resulting downloaded material is maintained in a 'safe store' and from a specific computer with a fixed IP address. This access is maintained open for a specific period of time, subject to ethical review. On the expiry of this period, access is stopped and any research data (or documents) available within it will be deleted.

---

*Approved by University Research Governance Committee, January 2017*

Queries to [rgoffice@sussex.ac.uk](mailto:rgoffice@sussex.ac.uk)

---

<sup>3</sup> Consisting of the Pro V-C for Research, the Director of Research and Enterprise and a C-REC Chair from a Committee that played no part in its initial ethical review.

<sup>4</sup> <http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/oversight-of-security-sensitive-research-material-in-uk-universities.aspx>