Guidance issued following consideration of the UUK paper on the
Oversight of security-sensitive research material in UK universities

Introduction

1. This advice for staff and students at the University of Oxford and visitors carrying out research at the University, hereafter ‘researchers’ for short, is issued in the context of statutory guidance by Government on the Prevent Duty. That guidance makes particular reference to a Universities UK paper concerned with ‘security-sensitive research material’ that might be gathered or generated relating to research which

(a) Is commissioned by the military; or

(b) Is commissioned under an EU security call; or

(c) Involves the acquisition of security clearances; or

(d) Concerns terrorist or extreme groups.

Category-specific requirements

2. **All research at the University in categories (a), (b) or (c) will require research contracts with third parties. Those contracts will normally specify in detail**

- Where and how research material can be accessed, analysed, stored or transmitted;
- Whether any of the material can lawfully be shared with other organisations, and if so, how; and
- How to report any actual or suspected information security breaches.³

Researchers must seek advice from Research Services if they propose to conduct research of this (or any other kind) under a contract (sometimes referred to as a research-related agreement).⁴ Research Services will discuss with the researchers the proposed terms and conditions and advise, where required, on sources of specialist advice and support in relation to e.g. data handling or information security.

Researchers carrying out such research will need to put in place and abide by strict information security protocols required under contract.

---

¹ Guidelines approved by the University of Oxford Research Committee, 26 January 2017
³ Research on work marked ‘UK Government Classified’, e.g., will come with a detailed Security Aspects Letter
⁴ Only the Director, Research Services or their delegate is authorised to sign research and research-related contracts and grant awards on behalf of the University.
4. **In relation to research in category (d)** – which ‘concerns terrorist or extreme groups’ – the University Research Committee (URC) resolved in June 2016 that no additional or special measures should be mandated. Such research should be conducted in compliance with existing University policies and procedures. The University of Oxford does not require research concerning ‘terrorist or extreme groups’ to be registered with or pre-approved by the University. Ethical review and approval must be obtained in advance of the research starting via the Central University Research Ethics Committee (CUREC) if the research involves human participants and personal data (see paragraph 5) and users of University IT or network facilities should comply with the provisions of the University’s *Regulations Relating to the use of Information Technology Facilities* (see paragraph 9ff).

5. **Research in category (d)** may involve external funding or access to data which is subject to specific research contracts/agreements – in those cases, the protocol is the same as described in paragraph (2) above.

**Human Research Ethics**

6. If your research involves human participants or the collection of personal data, you must abide by the policies established by the Central University Research Ethics Committee (CUREC). See [http://researchsupport.admin.ox.ac.uk/governance/ethics](http://researchsupport.admin.ox.ac.uk/governance/ethics). The University is committed to ensuring that its research activities involving human participants are conducted in a way which respects the dignity, rights, and welfare of participants, and which minimises risk to participants, researchers, third parties, and to the University itself. In accordance with its policy on research involving human participants and personal data, the University requires that all such research be subject to appropriate ethical review.

7. The CUREC checklists and application forms include questions asking how you will ensure that any personal or sensitive data are captured, transferred and stored securely. The University’s Research Data Team ([researchdata@ox.ac.uk](mailto:researchdata@ox.ac.uk)) can provide advice to research staff and students seeking advice on how to best to achieve this.

8. The handling of personal data must be in compliance with the University’s Guidance on Data Protection – see [http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/](http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/)

**Export Controls**

9. **Researchers have a personal legal obligation to carefully consider whether they need to apply for a licence from the UK Export Control Organisation (ECO) to ‘export’ goods, technology, software, designs or other related ‘know-how.’** There is a particular focus on any

   (a) Items that have been specially designed or modified for military use and their components

   (b) Dual-use items - those that can be used for civil or military purposes - which meet certain specified technical standards and some of their components
Technologies, material, equipment or know-how that could be used in nuclear, chemical, or biological weapons or ballistic missiles other explosive devices or their means of delivery.\(^5\)

Research in categories (a) to (c) above (cf. para 1) may well involve export control issues. For advice, see [http://researchsupport.admin.ox.ac.uk/policy/export](http://researchsupport.admin.ox.ac.uk/policy/export)

### University IT Regulations

10. The *University Regulations Relating to the use of Information Technology Facilities* state that the University provides computer facilities and access to its computer networks only for purposes directly connected with the work of the University and the colleges and with the normal academic activities of their members.

11. Section 7 of the Regulations state what users of the users of university IT or network facilities are not permitted to do.\(^6\) Users are not permitted e.g. to use university IT or network facilities for any ‘unlawful activity.’\(^7\)

12. The Regulations state that ‘Any individual responsible for the administration of any university or college computer or network system, or otherwise having access to data on such a system, shall comply with the provisions of the Information Security Policy and Data Protection Policy.’

### Information Security (physical and digital)

13. *If you are working to collect, analyse, store or in any other way use security-sensitive research material, you should have particular regard to information security.*

14. The first step is to ensure that you manage your research activities in line with the University’s information security policy. These requirements are provided in a [Baseline Assessment](http://researchsupport.admin.ox.ac.uk/policy/export) to allow you to measure your compliance with the policy.

15. It may then be necessary to conduct a risk assessment to determine whether additional security measures are needed. This process should identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

16. You may need to consider, with the help of your department (and where appropriate the central Info Sec Team), a range of security measures including e.g.

- the use of special (dedicated) servers with particular levels of security
- special access controls
- whether work should only be undertaken using designated networks

---

\(^5\) The University also has a system in place to ensure compliance with the Academic Technology Approval Scheme (ATAS) requirement where a certificate is required for nationals of some countries in order to study certain subjects in the UK

\(^6\) [http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml](http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml)

\(^7\) The Crown Prosecution Service (CPS) provides access to information on what constitutes unlawful use of network and IT facilities in the UK. See [http://www.cps.gov.uk/legal/a_to_c/communications_offences/](http://www.cps.gov.uk/legal/a_to_c/communications_offences/)
• encryption of data and/or communications
• how physical and digital material should be securely stored during and after your research
• how you will share materials or findings or communicate the research with other researchers at Oxford or at other institutions in the UK or abroad.

For information and advice please see https://www.infosec.ox.ac.uk/ and http://researchdata.ox.ac.uk/home/managing-your-data-at-oxford/storage-and-backup/

Support and guidance for departments and staff is offered by the central Information Security "InfoSec" team – see https://www.infosec.ox.ac.uk/what-we-do

Research with the UK government or UK government information

17. Government policy is that ‘EVERYONE who works with government … has a duty of confidentiality and a responsibility to safeguard any Her Majesty’s Government (HMG) information or data that they access, irrespective of whether it is marked or not ….‘ The Security classifications used by HMG indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification (see below). The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements.8

**HMG Security Classifications**

- **OFFICIAL**
  The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

- **SECRET**
  Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

- **TOP SECRET**
  HMG’s most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

The police, intelligence and security services

18. Researchers should be aware that the police, government intelligence and security services may monitor on-line or other forms of research or communication, where they have the legal right to do so. Subject to their assessment of risk or other factors, they may choose to monitor ‘security-sensitive research.’ Researchers who access web sites (including the ‘dark web’9) that might be associated with security-sensitive issues should

9 http://www.bbc.co.uk/guides/z9j6nbk
be aware that those sites may be particularly subject to such surveillance. Particular care should be taken when researching Proscribed organisations.¹⁰

19. Researchers based overseas or researchers travelling to overseas locations will need to abide by local laws and regulations in regard to security-sensitive research material and the collecting and holding of related material. It is the responsibility of the researcher to ensure that they familiarise themselves with these local rules prior to travelling or, if locally based, prior to starting research. Any risk assessment of such research should address related risks.

¹⁰ https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2
For further information

**Central University Research Ethics Committee (CUREC) - Human Participants in Research** - information about CUREC and the CUREC application process and related training and resources available to University researchers – http://researchsupport.admin.ox.ac.uk/governance/ethics

**University of Oxford Regulations Relating to the use of Information Technology Facilities** – http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

**Information Security at Oxford** – https://www.infosec.ox.ac.uk/

  - Data management planning
  - Ethical issues and data protection
  - Backup, storage and security
  - Organising your data


**University of Oxford Guidelines on Data Protection** – http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/

**University of Oxford Guidance on Export Control Legislation** – http://researchsupport.admin.ox.ac.uk/policy/export


**Crown Prosecution Service (CPS) information on what constitutes unlawful use of network and IT facilities** – http://www.cps.gov.uk/legal/a_to_c/communications_offences

**University of Oxford site on the Prevent Duty** – http://www.ox.ac.uk/staff/working_at_oxford/policies_procedures/prevent-duty