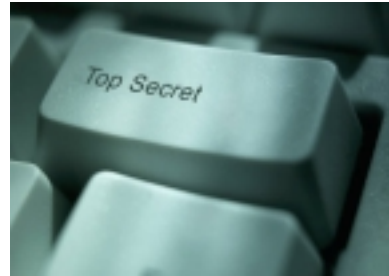




Research & Enterprise Services Bulletin

Bulletin No 007

Dated: March 2005



Official Secrets Acts – Important Information and Guidance

Why might I come into contact with these Acts?

Certain research and other projects in which the University is involved require adherence to the provisions of the Official Secrets Acts. The obligations placed on you and the University in such circumstances often involve very strict terms of confidentiality. Typically such projects occur from dealings with Crown Servants, or government contractors, such as, for example, the Met Office that is governed by the Ministry of Defence.

Why does this matter to me?

- **Personal Criminal Liability** - there is potential for this following the unlawful disclosure of protected information that is damaging to the national interest. This could conceivably occur through sloppy housekeeping such as failing to lock away protected information when it is not in use or from discussing disclosed information with unauthorised third parties.

Furthermore, protected information can sometimes be difficult to identify.

- **Prove your innocence** - the Acts reverse the burden of proof in many scenarios. In effect this means that you would have to find a way to prove your innocence if a damaging breach were to occur. If damage has occurred due to a breach of confidentiality then this may be especially difficult for you to prove since you have been made aware of your ongoing confidentiality obligations under these Acts.

What do I need to be aware of and what should I be doing?

In the yellow box below you will find an overview of what the Acts cover. In the red box you will find a useful practical list of recommended safeguards - if you have any questions or concerns about these please contact **Research and Enterprise Services** (RES) email: res@exeter.ac.uk telephone: ext 3456.

Official Secrets Act 1989

This Act states that it is an offence to disclose official information within six specified categories if the disclosure has damaged the national interest. Reasonable care must be taken to prevent unauthorised disclosure.

Penalties can extend to 2 years prison and/or a fine.

Official Secrets Act 1920

This Act deals with unauthorised admission to prohibited places and in particular the unauthorised use of uniforms, falsification of reports, impersonation and false documents. In addition it covers the disclosure or retention of official documents and communications with foreign agents and interfering with officers of the police or members of His Majesty's forces.

The burden remains on the accused in relation to establishing innocence for '*purpose[s] prejudicial to the safety or interests of the state*'.

Official Secrets Act 1911

This Act protects information useful to an enemy and places the burden on the accused to prove their innocence where it is alleged that they have undertaken a prohibited activity.

What should I be doing?

In order to protect **you** against the risk of personal criminal liability the safeguards detailed in the attached red box should be implemented for relevant projects. Key questions to ask yourself, with which RES can assist you, if you are at all unsure as to the answers, are:

- Who is the other party and are they a government organisation or a contractor working for a government organisation?
- Is my project covered by the Official Secrets Acts?
- If yes, has your project/contract been assessed by RES? (if not RES should be asked to assess the risks and obligations on your behalf)
- Are you properly aware of all of your obligations under the project/contract?
- Do you understand what needs to be done about these obligations?
- Has the status of the disclosed information been marked or otherwise confirmed in writing?
- Who can have access to the disclosed information?
- Will you need to visit the other party's site?

RECOMMENDED SAFEGUARDS FOR PROTECTING INFORMATION:

- All information disclosed to you under a relevant project should be treated as Secret unless it is otherwise classified in writing. This means that it cannot be further disclosed. It is worth asking the disclosing party to ensure that the information's status is confirmed in writing.
- You should always check whether the projects that you are working on are being undertaken subject to the provisions of the Official Secrets Act. This is especially important when the person disclosing is, or has received information from, a Crown servant or government contractor.
- Keep all disclosed information completely secure (unless it is clearly marked as being of a non-sensitive nature) and ensure that it is only disclosed to personnel authorised under the contract. This will involve but not be limited to the following activities:
 - Keeping all information locked away and not left on desktops or elsewhere when it is not being used.
 - Ensuring that all storage mechanisms (keys, passwords) are not accessible by unauthorised persons. This may include other members of staff.
 - Avoid displaying or revealing any disclosed information via any computing services including the Internet, intranets, portals or other online services.
 - Never send disclosed information by email.
 - Be aware of any special requirements governing document retention and disposal and put management systems in place to ensure that these (and other) obligations are adhered to.

RECOMMENDED SAFEGUARDS WHEN VISITING SENSITIVE SITES/PROHIBITED PLACES:

DO:

- Adhere rigorously to visitor procedures
- Ensure that you always have sufficient paperwork and passes to enable you to demonstrate that you are a bona fide visitor
- Remain in the proximity of site personnel at all times

DO NOT:

- Enter any restricted areas without appropriate clearance
- Do not keep records of any aspect of the visited site in any form
- Wander inadvertently into areas to which you have not been invited

What if someone sends me a contract involving these issues?

Please contact RES for specific advice in accordance with the contracts approval procedure outlined in RES bulletin 4.

What about security clearance?

Occasionally projects will require project personnel to undergo security clearance procedures (also known as vetting). The terms of the contract will specify if this is the case but it may not be easily apparent even if you are used to assessing contractual liabilities. This is because government and military organisations often refer to their standard conditions that then need to be obtained and understood. Once notified, RES will obtain the standard conditions for you (at any stage of collaborations but ideally at the outset) so that the University and those involved are fully apprised of their contractual obligations.

Useful Links

RES resources online:

<http://www.exeter.ac.uk/research/staff/>

MOD Website (Commercial Managers Toolkit):

<http://www.ams.mod.uk/ams/content/docs/toolkit/home.htm>

Acts of UK Parliament (as first enacted so not necessarily up to date):

<http://www.opsi.gov.uk/acts.htm>

And finally.... please remember: Any work involving Crown Servants or government contractors could potentially involve protected information so seek clarification at the outset. If you are visiting sensitive sites then be aware of the security procedures and site rules. If you are in any doubt as to your obligations, contact Claire Turner, Contracts Manager via:

re-contracts@exeter.ac.uk or via RES on 3456.