# Access by staff and students to security-sensitive material

## 1. Background and purpose of policy

Under the Counter-Terrorism and Security Act (2015) ("the Act"), section 26(I), the University has a duty, in exercising its functions, to have due regard to the need to prevent people from being drawn into terrorism (the 'Prevent' duty). The University's policy statement in relation to its Prevent duties is available at http://www.reading.ac.uk/web/FILES/student-and-academic-services/Prevent_Policy_Statement.pdf.

In having due regard to the Prevent duty, the University wishes to identify instances where security-sensitive materials are accessed by staff or students for purposes not related to University research or the study of a University programme. Given that a number of staff and students have a legitimate need to access security- sensitive material in the course of their studies or research, it is important that the University is aware of those individuals and the types of material which they may be accessing and takes appropriate steps to regulate the conditions under which it is accessed. If appropriate safeguards were not in place, members of staff and students accessing such materials might be vulnerable to arrest and prosecution or to being drawn into terrorism. The University therefore wishes to be in a position to confirm whether or not a member of staff or a student who is in possession of, or who is accessing, security-sensitive material has a good academic reason for doing so, and also to put in place arrangements which ensure that the security of such material is maintained, so that it is not accessed, inadvertently or otherwise, by those who are not prepared to view it.

The purpose of the policy set out below is therefore to enable research and study involving security-sensitive material to be undertaken, while safeguarding the researcher/student accessing the material, other students and staff, and meeting the University's obligations under the Act.

An outline of universities' obligations under the Act is available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

The University is also mindful of its obligations concerning freedom of speech and academic freedom. These are set out in the Code of Practice on Freedom of Speech (available at http://www.reading.ac.uk/web/FILES/Calendar/19.pdf) and the University's Charter of Incorporation (available at http://www.reading.ac.uk/web/FILES/calendar2016-17/Section_E_Charter.pdf) and nothing in this policy intends to limit freedom of speech or academic freedom within the law.

This policy also reflects the provisions set out in the University's IT Regulations for the Use of University of Reading's IT Facilities and Systems, available at:

http://www.reading.ac.uk/web/FILES/Calendar2015-16/Section_G_6_Regulations_for_the_Use_of_the_University_of_Reading's_IT_Facilities_and_Systems.pdf

3. **Scope**

This policy applies to all staff and students, who, as part of their academic work intend to access or are accessing security-sensitive material. 'Security-sensitive' material includes, but is not limited to:

- material which might be thought to encourage the commission, preparation or instigation of acts of terrorism,
- material which would be useful in the commission of acts of terrorism,
- material which glorifies acts of terrorism.

Security authorities may also consider material relating to animal rights extremism as falling within the definition security-sensitive material.

If you are in any doubt as to whether material you wish to access is considered to be security-sensitive, you should seek advice from:

(a) if you are an undergraduate or taught postgraduate student, the School Director of Teaching and Learning of the School responsible for the relevant module;

(b) if you are a postgraduate research student, your supervisor or School Director of Postgraduate Research Studies;

(c) if you are a member of staff undertaking academic or academic-related work, your Head of School; and

(d) exceptionally, if you are a member of staff undertaking other work where you may access security-sensitive material, your line manager or your Head of Function.

Undergraduate and taught postgraduate students are informed of this policy via internal communications and on the Reading University Student Essentials website http://student.reading.ac.uk/essentials. Postgraduate research students are informed of this policy in the Code of Practice for Research Students http://www.reading.ac.uk/web/FILES/qualitysupport/cop_resstudents.pdf and members of academic staff in https://www.reading.ac.uk/internal/res/ResearchEthics/reas-REethicshomepage.aspx.

Nothing in this policy supersedes or circumvents any requirement to seek from the Research Ethics Committee approval for research where such approval is normally required. The Research Ethics Committee will not grant approval to research that falls within the scope of this policy unless the process set out at paragraph 5 below has been followed.

## 4. Arrangements for access to security-sensitive material

Where a student or member of staff has good reason to access security-sensitive material for the purposes of their studies or research, he or she will be required to access such material only via a designated University-owned computer supported by the University's central IT Department. Access via any personally-owned device is not permitted. The provisions of the University's IT Regulations (see section 1 above) will apply in all cases.

Where a student or member of staff has good reason to store such sensitive material, only designated network-attached file storage services provided and managed by the central IT Department may be used for this purpose. Use of locally-attached or personally-owned file storage is not permitted. The University's IT Department must be consulted in such instances, and will need to understand for how long such material needs to be retained.

Where it is appropriate to do so, staff and students will be required to access such material in a secure setting, where the material cannot be accessed or inadvertently seen by other students. Details of that secure setting, or the arrangements for ensuring the material is not inadvertently or inappropriately disseminated, will be agreed. The material must not be shared or exchanged with persons other than the supervisor and other designated members of staff.

The provisions in the University's IT Regulations concerning the monitoring of IT facilities will apply in all instances: see Section 9 in http://www.reading.ac.uk/web/FILES/its/Section_G_6_Regulations_for_the_Use_of_the_University_of_Reading's_IT_Facilities_and_Systems_01.pdf.

Staff and students are required to confirm their assent to the arrangements set out in the IT Regulations before any material is accessed.

Students and staff are reminded that, as part of their research, they may view distressing material. The University takes seriously its obligations to safeguard the wellbeing of its students and staff. Students may access support via the Counselling and Wellbeing Service, should they wish to do so. Students will also be required to discuss their work or research with their supervisor or equivalent, and will be encouraged to raise any concerns at the earliest opportunity in order that the University can provide appropriate and reasonable support. Staff may access support via the employee assistance programme, details of which can be obtained from the HR webpages. Staff are also encouraged to speak to their manager or Head of School.

***Material which may fall outside the established law***

The University makes a distinction between security-sensitive material which may interact with its obligations concerning the Prevent duty, and that material which may also contravene the established law.

If anyone involved in the operation of this policy, whether those making a request, those considering it or any other party, is concerned that access to the material may contravene the established law, such concerns must be made known to the Teaching and Learning Dean or the Dean for Postgraduate Research Studies. He or she will seek appropriate advice, which may be from external organisations, before determining whether the material may be accessed.

## 5. Process

### 5.1 *Undergraduate and taught postgraduate students*

The following process must be followed in all cases where an undergraduate or taught postgraduate student wishes to access security-sensitive material for the purposes of their studies or research:

a) At the earliest opportunity, the student must consult the School Director of Teaching and Learning of the School responsible for the relevant module, and outline the intended topic for research, its rationale, and indicate the websites or other materials likely to be accessed. It is understood that this may change during the research project or relevant period of study, in which case the student must notify the School Director of Teaching and Learning of the changed parameters and the reason for the change (see (f) below).

b) Following this consultation, the student is required to submit to the School Director of Teaching and Learning the form 'Access to security-sensitive material', which requires information on:

   - the subject and scope of research
   - an indicative list of material to be accessed.

   The student will be required to confirm assent to the conditions which will apply to accessing the material, including the requirement that only designated University-owned IT equipment may be used for accessing and/or storing such material, that the material can only be accessed in a secure environment/in an agreed manner, that the material cannot be shared or exchanged, and that the access to materials will be monitored.

c) The School Director of Teaching and Learning considers and, if appropriate, recommends to the designated Teaching and Learning Dean (being at the date of this policy Dr David Carter whose email address is d.m.carter@reading.ac.uk) for whom the other Teaching and Learning Deans serve as alternates, approval of research into the topic and access to websites of a sensitive nature. The Teaching and Learning Dean will consider and, if appropriate, approve the recommendation, and will forward the signed form to the Prevent Duty Compliance Officer (being at the date of this policy Jack Paulley whose email address is j.paulley@reading.ac.uk) who will forward a copy of the form to the Director of IT.

d) The Prevent Duty Compliance Officer informs the student of the Teaching and Learning Dean's decision, the arrangements for accessing and/or storing security-sensitive material, the conditions which apply to accessing security-sensitive material, and the consequences of breaching the conditions. The following conditions will normally apply:

   i. Security-sensitive material will be accessed through, and stored on, designated University-owned IT equipment supported by the University's central IT Department, and not on any personally-owned device or locally-attached storage;

   ii. the material will be viewed in a secure, or other agreed, setting, where the material cannot be accessed by other students;

   iii. the material must not be shared or exchanged with persons other than the supervisor and other designated members of staff;

   iv. printed material of a sensitive nature must be held in a secure place

   v. the provisions of the University's IT Regulations (Section 9) relating to Monitoring will apply;

   vi. the student's arrangements for holding and accessing material and the material accessed online may be audited by the University Security Manager, and the audit may involve interviews with the student and/or supervisor;

   vii. the University may share information with the Higher Education Funding Council for England (HEFCE), Office for Students, Counter-Terrorist Unit and other relevant authorities, where it is lawful and appropriate for it to do so.

e) The Prevent Duty Compliance Officer records the decision on a dedicated database and enters a note on the SPR Notes field on RISIS stating 'Approved to access security-sensitive material; if necessary, contact the Prevent Duty Compliance Officer'. The record and associated documentation is retained for a period of 6 years from the point of termination of the relationship with the student, unless a longer period of retention is required by law, any other relevant legislation, or by order of a court.

f) If the intended scope of the research and access to security-sensitive material changes during the research project or relevant period of study, the student must immediately notify the School Director of Teaching and Learning of the changed parameters and the reason for the change. The decision to permit access to security-sensitive material will be reviewed.

g) In the event that a student breaches the conditions for access to security-sensitive material, the Teaching and Learning Dean may determine that consent for the access to security-sensitive material be withdrawn, which may

entail the student not being able to continue with the research topic. If such breaches also contravene the University's IT Regulations the provisions in those Regulations regarding infringement will also apply.

5.2 ***Postgraduate research students***

The following process must be followed in all cases where a postgraduate student wishes to access security-sensitive material for the purposes of their studies or research:

a) At the earliest opportunity, the student must consult his or her supervisor or School Director of Postgraduate Research Studies, and outline, in relation to the larger research topic, the rationale for accessing security-sensitive material, and indicate the websites or other materials likely to be accessed. It is understood that this may change during the research project, in which case the student must notify his or her supervisor and School Director of Postgraduate Research Studies of the changed parameters and the reason for the change. In this event, the decision to permit access to security-sensitive material will be reviewed.

b) Following this consultation, the student is required to submit to the School Director of Postgraduate Research Studies the form 'Access to security-sensitive material', which requires information on:

   - the subject and scope of research
   - an indicative list of material to be accessed.

   The student will be required to confirm assent to the conditions which will apply to accessing the material, including the requirement that only designated University-owned IT equipment may be used for accessing and/or storing such material, that the material can only be accessed in a secure environment/in an agreed manner, that the material cannot be shared or exchanged, and that the access to materials will be monitored.

c) The School Director of Postgraduate Research Studies considers and, if appropriate, recommends to the Dean of Postgraduate Research Studies (with a designated Teaching and Learning Dean acting as an alternate), approval of research into the topic and access to material and websites of a sensitive nature. The Dean of Postgraduate Research Studies will consider and, if appropriate, approve the recommendation, and will forward the signed form to the Prevent Duty Compliance Officer (being at the date of this policy Jack Paulley whose email address is j.paulley@reading.ac.uk), who will forward a copy of the form to the Director of IT.

d) The Prevent Duty Compliance Officer informs the student of the decision of the Dean of Postgraduate Research Studies, and the arrangements for accessing and/or storing security-sensitive material, the conditions which apply to accessing security-sensitive material, and the consequences of breaching the conditions. The following conditions will normally apply:

i. Security-sensitive material will be accessed through, and stored on, designated University-owned IT equipment supported by the University's central IT Department, and not on any personally-owned device or locally-attached storage;

ii. the material will be viewed in a secure, or other agreed, setting, where the material cannot be accessed by other students;

iii. the material must not be shared or exchanged with persons other than the supervisor and other designated members of staff;

iv. printed material of a sensitive nature must be held in a secure place

v. the provisions of the University's IT Regulations (Section 9) relating to Monitoring will apply;

vi. the student's arrangements for holding and accessing material and the material accessed online may be audited by the University Security Manager, and the audit may involve interviews with the student and/or supervisor;

vii. the University may share information with the Higher Education Funding Council for England (HEFCE), Office for Students, Counter-Terrorist Unit and other relevant authorities, where it is lawful and appropriate for it to do so.

e) The Prevent Duty Compliance Officer records the decision on a dedicated database and enters a note on the SPR Notes field on RISIS stating 'Approved to access security-sensitive material; if necessary, contact Prevent Duty Compliance Officer'. The record and associated documentation is retained for a period of 6 years from the point of termination of the relationship with the student, unless a longer period of retention is required by law, any other relevant legislation, or by order of a court.

f) If the intended scope of the research and access to security-sensitive material changes during the research project or relevant period of study, the student must immediately notify the School Director of Postgraduate Research Studies of the changed parameters and the reason for the change. The decision to permit access to security-sensitive material will be reviewed.

g) In the event that a student breaches the conditions for access to security-sensitive material, the Dean of Postgraduate Research Studies may determine that consent for the access to security-sensitive material be withdrawn, which may entail the student not being able to continue with the research topic. If such breaches also contravene the University's IT Regulations the provisions in those Regulations regarding infringement will also apply.

5.3 ***Staff***

The following process must be followed in all cases where a member of staff wishes to access security-sensitive material for the purposes of their preparation of teaching or their research:

a) The member of staff is required to submit to Head of School the form 'Access to security-sensitive material', which requires information on:

   - the subject and scope of research
   - an indicative list of material to be accessed.

   The member of staff will be required to confirm assent to the conditions which will apply to accessing the material, including the requirement that only designated University-owned IT equipment may be used for accessing and/or storing such material, that the material can only be accessed in a secure environment/in an agreed manner, that the material cannot be shared or exchanged, and that the access to materials will be monitored.

b) The Head of School considers and, if appropriate, recommends to the Dean of Postgraduate Research Studies (with a designated Teaching and Learning Dean acting as an alternate), approval of research into the topic and access to material and websites of a sensitive nature. The Dean of Postgraduate Research Studies will consider and, if appropriate, approve the recommendation, and will forward the signed form to the Prevent Duty Compliance Officer (being at the date of this policy Jack Paulley whose email address is j.paulley@reading.ac.uk), who will forward a copy of the form to the Director of IT.

c) The Prevent Duty Compliance Officer informs the member of staff of the decision of the Dean of Postgraduate Research Studies, the arrangements for accessing and/or storing security-sensitive material, the conditions which apply to accessing security-sensitive material, and the consequences of breaching the conditions. The following conditions will normally apply:

   i. Security-sensitive material will be accessed through, and stored on, designated University-owned IT equipment supported by the University's central IT Department, and not on any personally-owned device or locally-attached storage;

   ii. the material will be viewed in a secure, or other agreed, setting, where the material cannot be accessed by other students;

   iii. the material must not be shared or exchanged with other persons unless specific permission has been given;

   iv. printed material of a sensitive nature must be held in a secure place

   v. the provisions of the University's IT Regulations (Section 9) relating to Monitoring will apply;

vi. the member of staff's arrangements for holding and accessing material and the material accessed online may be audited by the University Security Manager, and the audit may involve interviews with the member of staff;

vii. the University may share information with the Higher Education Funding Council for England (HEFCE), Office for Students, Counter-Terrorist Unit and other relevant authorities, where it is lawful and appropriate for it to do so.

d) The Prevent Duty Compliance Officer records the decision on a dedicated database. The record and associated documentation is retained for a period of 6 years from the point of termination of the relationship with the member of staff, unless a longer period of retention is required by law, any other relevant legislation, or by order of a court.

e) If the intended scope of the research and access to security-sensitive material changes during the research project or relevant period of study, the member of staff must immediately notify the Head of School of the changed parameters and the reason for the change. The decision to permit access to security-sensitive material will be reviewed.

f) In the event that a member of staff breaches the conditions for access to security-sensitive material, the Dean of Postgraduate Research Studies may determine that consent for the access to security-sensitive material be withdrawn, which may entail the member of staff not being able to continue with the research. If such breaches also contravene the University's IT Regulations the provisions in those Regulations regarding infringement will also apply.

g) Members of the Vice-Chancellor's Office, if acting in their capacity as an academic member of staff, will follow the process set out above by which they are required to submit to the relevant Head of School the form 'Access to security-sensitive material'. Otherwise, a member of the Vice-Chancellor's Office must get approval from the Vice-Chancellor. In the event that the Vice-Chancellor wishes to access security-sensitive material, he must obtain approval from the President of Council.

## 6. Appeals

A student or member of staff who wishes to appeal against the decision of the Teaching and Learning Dean or Dean of Postgraduate Research Studies in relation to access to security-sensitive material should submit a statement explaining the basis of their appeal to the Student Appeals and Academic Misconduct Officer (being at the date of this policy Claire Hall whose email address is c.hall@reading.ac.uk) Claire Hall. The appeal will be determined, in the case of a student (including postgraduate research students), by the Pro-Vice Chancellor (Teaching and Learning) and, in the case of a member of staff, the Pro-Vice-Chancellor (Research and Innovation). Other Pro-Vice-Chancellors act as alternates.

## 7. Monitoring

The student's or member of staff's arrangements for holding and accessing material and the material accessed online will be audited by the University on at least a quarterly basis.

8. **Training**

Training in the Prevent duties, as they relate to access to security-sensitive material, is provided to all those with responsibilities under this policy.

If you have any queries in relation to the applicability of this policy to your research or other work, please contact those indicated in section 3(a)-(d) above. If you have queries in relation to the policy more broadly, please contact Keith Swanson, Director of Quality Support and Development (k.h.s.swanson@reading; extension 4488).

| VERSION | SECTION | KEEPER | REVIEWED | APPROVING AUTHORITY | APPROVAL DATE | START DATE | NEXT REVIEW |
|---|---|---|---|---|---|---|---|
| 1.0 | AGS | The University Secretary | Annually | UEB | 03/10/16 | 03/10/16 | 01/09/17 |