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 Approach to the Prevent Duty is available here.

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 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 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.

The application of this policy relies on academic staff exercising their academic judgement and drawing on the wider support available in the University to interpret its provisions as they relate to individual circumstances.

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 and the University's Charter of Incorporation and nothing in this policy is intended 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.

2. 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' does not have a given legal definition, but, for the purposes of this policy, security-sensitive material includes, but is not limited to:

- material which could reasonably be thought to encourage, in present circumstances, the commission, preparation or instigation of acts of terrorism by individuals being exposed to such materials,
- material which would be useful in the commission of acts of terrorism,
- material which glorifies acts of terrorism as conduct which should be emulated in present circumstances by individuals exposed to such materials.

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

Material that is clearly intended as part of an academic debate or critical engagement with terrorism and violence, be it theoretical, historical, or empirical, should normally not be considered to be security-sensitive.
Equally material which relates to historical advocacy of terrorism or unlawful violence should normally not be considered security-sensitive.

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. Postgraduate research students are informed of this policy in the Code of Practice for Research Students and members of academic staff in https://www.reading.ac.uk/internal/academic-and-governance-services/research-ethics/RECethicshomepage.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.

3. Arrangements for access to security-sensitive material

Where a student or member of staff has good reason to access or store security-sensitive material, they should first discuss the matter with their School Director of Teaching and Learning (in respect of taught programmes), School Director of Postgraduate Research Studies (in respect of postgraduate research programmes) or Head of School (in respect of members of staff).

Where approval is given for students or staff to access security-sensitive material, the following conditions will normally apply:

a. security-sensitive material will be accessed in line with the Regulations for the use of the University of Reading's IT Facilities and Systems. The provisions in the University's IT Regulations concerning the monitoring of IT facilities will apply in all instances;

b. security-sensitive material will be accessed in an appropriate location where it will not be inadvertently seen by students or staff in order to avoid the material causing undue alarm and to mitigate risks arising under the Prevent duty;

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

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

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

f. the University may share information with the Office for Students, Counter-Terrorist Unit and other relevant authorities, where it is lawful and appropriate for it to do so.

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 are also required to discuss their studies or research with the relevant module convener or 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 Head of School and they will seek appropriate advice, which may be from external organisations, before determining whether the material may be accessed.

4. Process

4.1 An individual who wishes to access security-sensitive material for the purposes of their studies or research is responsible for completing and submitting an application to access such material, except in those cases where a module convener has registered the relevant module as involving access to security-sensitive material (as specified in section 4.2 below).

Sub-sections provide information on the process where:

- students on a module may reasonably be expected to access security-sensitive material (4.2)
- students individually wish to access security-sensitive material for studies/research (4.3)

- staff wish to access security-sensitive material (for research or other work-related purposes) (4.4).

There is a strong presumption that, where a member of academic staff considers that security-sensitive material is relevant to, and appropriate for, studies or research at the University, access to such security-sensitive materials will be approved unless a specific concern is evident.

4.2 ***Where students on a module may reasonably be expected to access security-sensitive material***

(a) Where there is a reasonable expectation that, for the purposes of studying a module, students may access security-sensitive material, the module convener 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

at least one month before the beginning of the module's delivery or before the point at which a student might be expected to access material for the module, whichever is sooner. If the SDTL or the Head of School has any concerns about students' accessing such material while studying the module, they will discuss the matter with the module convener.

(b) The School Director of Teaching and Learning considers the application and makes a recommendation to the Head of School, which may be:

(i) the material referred to in the application is not security-sensitive and therefore approval for access is not required;

(ii) the material is security-sensitive and access to the material is approved on the grounds that the material is relevant to, and appropriate for, the purposes of study or research;

(iii) the material is security-sensitive and access to the material is not approved on the grounds that the material is not relevant to, or appropriate for, the purposes of study or research.

The Head of School will consider and make a decision in respect of the application in the light of the recommendation. In the case of (i), the Head of School will inform the module convener; in the case of (ii) and (iii), the Head of School 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). In the absence of a Head of School, the Teaching and Learning Dean with responsibility for the School may act on behalf of the Head of School.

Brief guidance on considering applications for access to security-sensitive material is given in section 4.5 below. The School Director of Teaching and Learning and the Head of School should consult the Prevent Duty Compliance Officer and/or a Teaching and Learning Dean if they wish for further guidance on the policy and its interpretation in the context of an application.

(c) Approval for access to security-sensitive material in respect of a specified module remains in place for a period of five years, but module conveners should keep the status of material under review in the light of changing circumstances and context.

(d) The Prevent Duty Compliance Officer records the decision on a dedicated database.

(e) Where access has been approved, it is the responsibility of the module convener to ensure that students taking the module are:

(i) informed that the module has been registered as requiring possible access to security-sensitive material for the specified module and that they therefore do not need to register individually to access security-sensitive material for this module;

(ii) informed of the conditions which apply to accessing security-sensitive material, the consequences of breaching the conditions, and the support available, as set out in section 3 of this policy.

The module convener must inform students in writing of (i) and (ii) above, via their University email account, at a point before the students might be expected to access material for the module; this may be shortly after their registration for the module, or at the point when a reading list is made available, or in the first week of the module's delivery. If students have been informed before the start of the module, they should be reminded of the provisions in the first week of delivery and subsequently if the provisions are particularly relevant to material covered in a forthcoming class. This is a duty of care to ensure that the requirements of the policy are met and that safeguarding arrangements are in place for the benefit of the student.

(f) In the event that a student breaches the conditions for access to security- sensitive material, the Head of School 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 topic. If such breaches also contravene the University's IT Regulations the provisions in those Regulations regarding infringement will also apply.

4.3 ***Where students individually wish to access security-sensitive material for studies/research***

(a) The following provisions apply to all students, including postgraduate research students, unless they have been notified that their access to security-sensitive material is covered by the provisions of section 4.2 above. It should be noted that the provisions of section 4.2 are effective only for the module specified and not for material they may wish to access for their studies or research in respect of other modules.

(b) Where a student wishes to access security-sensitive material for the purposes of study or research, the student must consult at the earliest opportunity:

- *For undergraduate and taught postgraduate students*
  School Director of Teaching and Learning of the School responsible for the relevant module
- *For postgraduate research students*
  their supervisor or School Director of Postgraduate Research Studies

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

(c) Following this consultation, the student is required to submit to the School Director of Teaching and Learning/ 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.

(d) The School Director of Teaching and Learning/ School Director of Postgraduate Research Studies considers the application and makes a recommendation to the Head of School, which may be:

(i) the material referred to in the application is not security-sensitive and therefore approval for access is not required;

(ii) the material is security-sensitive and access to the material is approved on the grounds that the material is relevant to, and appropriate for, the purposes of study or research;

(iii) the material is security-sensitive and access to the material is not approved on the grounds that the material is not relevant to, or appropriate for, the purposes of study or research.

The Head of School will consider and make a decision in respect of the application in the light of the recommendation. In the case of (i), the Head of School will inform the student; in the case of (ii) and (iii), the Head of School 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). In the absence of a Head of School, the Teaching and Learning Dean with responsibility for the School may act on behalf of the Head of School.

Brief guidance on considering applications for access to security-sensitive material is given in section 4.5 below. The School Director of Teaching and Learning and the Head of School should consult the relevant module convener and/or dissertation supervisor and/or Programme Director in respect of the relevance of the material to the student's studies or research, and should consult the Prevent Duty Compliance Officer and/or a Teaching and Learning Dean if they wish for further guidance on the policy and its interpretation in the context of an application.

(e) The Prevent Duty Compliance Officer informs the student of the Head of School's decision, the conditions which apply to accessing security-sensitive material, the consequences of breaching the conditions, and the support available to students.

(f) 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 six 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.

(g) 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/ School Director of Postgraduate Research Studies of the changed parameters and the reason for the change. The decision to approve access to security-sensitive material will be reviewed.

(h) In the event that a student breaches the conditions for access to security- sensitive material, the Head of School may determine that consent for the access to security-sensitive material be withdrawn, which may have consequences for their studies or 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.

4.4 ***Where staff wish to access security-sensitive material (for research or other work-related***

purposes)

(a) 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.

(b) The member of staff is required to submit to the 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 apply to accessing the material.

(c) The Head of School considers the application and determines whether:

(i) the material referred to in the application is not security-sensitive and therefore approval for access is not required;

(ii) the material is security-sensitive and access to the material is approved on the grounds that the material is relevant to, and appropriate for, the purposes of study or research;

(iii) the material is security-sensitive and access to the material is not approved on the grounds that the material is not relevant to, or appropriate for, the purposes of study or research.

In the case of (i), the Head of School will inform the member of staff of the decisions; in the case of (ii) and (iii), the Head of School 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).

Brief guidance on considering applications for access to security-sensitive material is given in section 4.5 below. The Head of School should consult the Prevent Duty Compliance Officer (who may refer the inquiry to a Research Dean or Teaching and Learning Dean) if they wish for further guidance on the policy and its interpretation in the context of an application.

(d) The Prevent Duty Compliance Officer formally informs the member of staff of the decision of the Head of School, the conditions which apply to accessing security-sensitive material, the consequences of breaching the conditions, and the support available.

(e) 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.

(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 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.

(g) In the event that a member of staff breaches the conditions for access to security-sensitive material, the Head of School may determine that consent for the access to security-sensitive material be withdrawn. If such breaches also contravene the University's IT Regulations the provisions in those Regulations regarding infringement will also apply.

(h) 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.

4.5 ***Guidance on considering applications for access to security-sensitive material***

In considering an application, the School Director of Teaching and Learning//School Director of Postgraduate Research Studies and the Head of School should have regard to the relevance of the cited security-sensitive material for the work of the student or member of staff. This will require the exercise of judgement and this guidance cannot provide detailed criteria by which to determine each case. However, in order to guide the interpretation of the policy and the judgement of those responsible, an example may be helpful. For example, it would be reasonable to agree that a student whose research topic was toxin production could legitimately access material on anthrax production since this is relevant to their research. If, however, a student whose study or research bore no relation to anthrax production (for example, a topic on political philosophy), a request to access such an article would not seem well-founded and would reasonably be declined.

5. Appeals

A student or member of staff who wishes to appeal against the decision of the Head of School 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 Rachel Willis whose email address is r.willis@reading.ac.uk). The appeal will be determined, in the case of a student (including postgraduate research students), by a designated Teaching and Learning Dean (with other Teaching and Learning Deans acting as alternates), and, in the case of a member of staff, the Pro-Vice- Chancellor (Research and Innovation) (with other Pro-Vice-Chancellors acting as alternates). Those responsible for hearing the appeal must not have had any prior involvement in the case.

6. 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:

Relevant School Director of Teaching and Learning
Relevant School Director of Postgraduate Research Studies
Relevant Head of School
Relevant Teaching and Learning Dean
Prevent Duty Compliance Officer.

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
1.0	AGS	The University Secretary	Annually	UEB	03/10/16
2.0	AGS	The University Secretary	Annually	UEB	23/10/17
3.0	AGS	The University Secretary	Annually	UEB	23/09/19