University of Exeter

Access to Restricted Materials Policy and Justification Process

Version	Update
1.0	Current version on internet (23/07/2025) no approval date
1.1	Updated to draft 1.1. to include a justification process and application digital form (Dec 2025 for consultation)
1.2	For approval post consultation, Feb 2026
1.3	Approved

Approval Route and dates	
V1.1 **Prevent Compliance Committee, October 2025** **Compliance Committee, virtual consultation, REIC.** **V1.3 Compliance Committee**	 **December 2025** **January 2026** **February 2026 - APPROVED**
Authors	**Kate Lindsell and Chrysten Cole**

1.0 Introduction

1.1 Staff or students may require access to information which could be construed as illegal, raise suspicion of criminality or potentially be in breach of the Regulations relating to the Use of Information Technology Facilities.

1.2 The University recognises the importance of research and education, but also acknowledges the risks involved in accessing such material and has developed this code of conduct, including an approval process, to protect the individual and University.

1.3 This process is designed to protect staff and students accessing such material by adhering to this code and notifying the University of the intention to access such materials relevant so that justification can be officially granted, support can be provided, and access can be logged.

1.4 Material includes, but is not limited to:

- material which might be considered as useful in the commission, preparation or instigation of acts of terrorism, material which would aid or support in the commission of acts of terrorism, material which glorifies acts of terrorism.
- Material that could be harmful should it be lost, stolen or mishandled
- Materials that are considered illegal
- Security authorities may also consider material relating to animal rights extremism as falling within the definition security-sensitive material.

1.4 This policy is concerned with restricted materials. All IT users should be fully aware of the university policies and procedures regarding acceptable use of IT equipment. https://www.exeter.ac.uk/staff/policies/calendar/part1/otherregs/its/

2.0 Legal basis and Scope of policy for access to restricted materials

2.1 This Policy applies any member of staff or student who, due to legitimate research or education-based reasons would like to seek justification to access materials that could be construed as illegal or raise suspicion of criminality by the police or security forces.

2.2 It is an offence to:

- collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism; or
- to possess a document or record (including a photographic or electronic record) containing information of that kind (i.e. any document that would provide practical assistance to a person committing or preparing for an act of terrorism e.g. an Al Qaeda training manual); or
- disseminate terrorist publications if they are distributed, circulated, transmit electronically, sold / loaned / given a terrorist publication, provide a service to enable others to obtain a terrorist publication or have in their possession a terrorist publication with the intention of transmitting, etc, it; and/ or. For this offence to be committed, the individual must have the intention to encourage or induce others, directly or indirectly, or to help others to commit or to prepare for acts of terrorism.

2.3 A terrorist publication includes electronic publications and is any matter that may be understood by the recipients as providing encouragement or inducement to commit or prepare for terrorist acts and which is understood by the recipients to be made available to them wholly or mainly for the purposes of being so useful to them.

3.0 Obtaining justification for access to restricted materials

3.1 All requests to have justification for access restricted materials must be made through the official process, which can be evidenced in the event that there is any dispute over criminal intention.

3.2 Where there is a risk of accessing information which could be considered criminal, it may be a defence for the person to prove that he / she/ they had a reasonable excuse. It will assist any

concerns being raised about criminal activity if the relevant member of staff or student show that accessing the materials/ sites and/ or keeping the record was required for the purpose of pursuing the particular academic course or research and for no other more ambiguous purposes.

3.3 The ease with which this can be proved will depend on the clarity with which the research or the course and its training objectives have been drafted.

3.4 In seeking to obtain justification for access to restricted materials, it is important therefore to identify:

- the sites that provide a useful learning tool and ensure that the access is limited to these sites
- the people who will be accessing the material
- the basis on which the material will be used
- the process for retaining access records, where the data would be kept, whether it is necessary to keep a record for the purposes of achieving the research or learning outcomes (e.g. is it necessary for completing coursework?); and
- what retention process is in place regarding accessed materials, and when these will be destroyed.

3.5 Where access to materials which may be criminal would occur, restrictions on any subsequent dissemination of such materials should also be constrained. However, it is worth exercising caution by making the purposes of the research or education clear and prohibiting any further dissemination of these publications by staff or students.

3.6 This is a challenging area because any guidance is an attempt to anticipate the methods of police / MI5 and other enforcement authorities.

3.7 The law is strict, and the very fact of possessing or disseminating restricted material may be enough to warrant an investigation by the police, and a member of staff or student would be put in the position of having to advance a credible defence. If there is a clear link between learning outcomes and any information downloaded / disseminated, then the police may be reluctant to pursue the matter, though this cannot be guaranteed.

3.8 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 legal@exeter.ac.uk or follow the approval process and await advice.

3.9 Following this policy and completing an Access to Restricted Materials Request Form will evidence that appropriate review and justification for such access has been sought.

3.10 Not all applications will be agreed.

3.11 justification does not exempt staff/ students from any future criminal proceedings but, with this justification, the individual will be able to confirm that it had been considered for research purposes and with relevant controls.

3.12 Justification will be considered for UK based data, accessed within the UK only.

4.0 Roles and Responsibilities

4.1 **The University General Counsel and Assistant Director Assurance Compliance and Risk:**

- will ensure that the policy in in place and up to date
- will ensure that the process for applications is in place and justification requests are processed effectively, with advice from the DPO as required.
- that escalations are made in respect of justifications for high-risk applications and outcomes are logged

4.2 **Persons seeking approval**

- will ensure that data is accessed, used and stored within the limit of the justification. possessing or disseminating restricted material may be enough to warrant an investigation by the police, and a member of staff or student would be put in the position of having to advance a credible defence. If there is a clear link between learning outcomes and any information downloaded / disseminated, then the police may be reluctant to pursue the matter, though this cannot be guaranteed.
- will be responsible for handling data in safe matter and not allowing access to others
- will raise concerns regarding safety and security of the data immediately, by contacting legal services
- Any lost, stolen or concerns about data security must be reported immediately to the Information Governance Team informationgovernance@exeter.ac.uk.

4.3 **Those approving access to restricted materials at local level (Supervisors of staff/ students who are making an application for access)**

- will ensure that they understand the reasons for the request and can justify the need for access
- will ensure that proposed arrangements for accessing, handling and storing data are suitable, taking advice from the Information Governance Team as required
- will ensure that they routinely monitor those will access, to ensure that access rules are not breached and that any health and wellbeing concerns are managed
- they will escalate any concerns regarding restricted materials to legal services immediately.
- Any lost, stolen or concerns about data security must be reported immediately to the Information Governance Team informationgovernance@exeter.ac.uk.

5.0 Process for gaining justification for use of restricted materials

All persons wishing to seek justification shall follow all steps in the process and responsibilities outlined below.

5.1 Staff wishing to apply for justification for access restricted materials will:

- Gain approval from their supervisor/ line manager for the work, giving specific examples / list of materials you will be accessing and reasons for this.
- If permission is given by the line manager/ supervisor, the online application can be submitted . This must include the name of the line manager / supervisor.
- All sections of the form must be completed in order for the application to be considered.

The applicant is responsible for ensuring that the information provided on the form is accurate.

- The application form is found here Access to Restricted Materials Request – Fill in form

5.2 Students wishing to apply for justification for access to restricted Materials

- Gain approval from the PI / Supervisor
- The application for approval must be submitted with supporting written evidence from the supervisor / PI that approval has been granted.

5.3 **1st line approver**- Appropriate representatives from each of Legal and Compliance and Risk will:

- Receive the completed application form.
- Follow up with the applicant for more details if required.
- Assess the risk and assign a risk score (High or low) based on the type of materials that are being requested.
- The below risk matrix will be used to consider each application, and each application will be considered on a case-by-case basis:

High	Low
Illegal materials or materials that would require significant justification	Materials that could be on the margins of legal, but would require formal justification to support an enquiry

- Recommended for justification from the approvers adding conditions as required.

5.4 Senior Approvers

- Justification will be sought from the Senior Vice President, Registrar and Secretary and Senior Vice President, Provost and PVC for any high-risk application and return their outcome to the 1st Approver.
- General Counsel and Director of Legal and Student Cases justification for any GREEN applications who will return their opinion to the 1st Approver.

5.5 Justified Cases

- justifications requests will be recorded in the central system, within the Legal Team and the applicant will be informed of the outcome.
- It is the responsibility of the applicant to follow the requirements of the justified application. They must ensure that all risk management arrangements that were include in the approved application are implemented.

- The Information Security Team will be informed of any justifications. They are responsible for alerting JANET Security team (JANET CSIRT) to inform them that the activity is being undertaken and that staff and / or students will gain access to terrorist and other controversial websites during this work. Since courses such as this are provided in other universities, and to some extent analysing terrorist materials is also a genuine academic pursuit, this will not be uncharted territory for JANET. However, unless the notification is provided, the activities may be construed as a breach of the JANET Acceptable Use Policy (www.ja.net/company/policies/aup.html), though specific provision is not made for terrorist sites.

- If any changes are required to the approved application, these must follow the same process, and the application must be re-submitted, highlighting the changes required.

- Justified cases will be time limited, and the applicant will be set an end date. Continuing beyond the end date will require an extension.

- if applicants are within the deadline, but no longer require access, they must update the 1st line approver.

5.6 Record Keeping requirements

- The form detailing the conditions, access details, approval and retention schedule will be kept centrally for a time period deemed appropriate for the application, normally 7 years.

- The person responsible for the materials (listed on the MS form) will be responsible for the security and safety of the restricted materials including controlling any access on an ongoing basis. This includes:

    - Not disseminating materials digitally to others

    - Do not screenshot or save images

    - do not share information relating to how to access publicly available sites which contain restricted materials

- The person responsible for the materials (named on the MS form) will be responsible for the data retention schedule and will dispose securely of records in accordance with approval.

5.7 Data Breaches

- Any lost, stolen or concerns about data security must be reported immediately to the Information Governance Team informationgovernance@exeter.ac.uk.

- Information Governance will investigate the incident and act as required.

5.0 Information, training and assessment

5.1 the TRF pre award risk assessment, part of the Worktribe system, includes information and instruction on the requirement to apply for justification to access restricted materials

5.2 the PI / Researcher information hub includes information on the process and policy for access to restricted materials

5.3 the University Prevent webpages and IT B - Regulations Relating to the Use of Information Technology Facilities refer to the Access to Restricted information policy and process.

6.0 Audit and Compliance

6.1 The General Counsel, supported by the Assistant Director of Assurance, Compliance and Risk will periodically check that projects are / have been managed in accordance with approval. The results will be reported to the Prevent Compliance Committee annually.

6.2 Failure to demonstrate compliance with approval conditions could result in HR proceedings Research Misconduct investigations, student disciplinary proceedings or police investigations, as relevant.

Appendix 1: Questions on the application form

- Title of project
- Name of Supervisor / line manager
- Email address for supervisor
- Department you are working in for this research project
- Please list the names of any academics you are collaborating with for this work and state if they are external to the University of Exeter
- Will you be working with any students (including PG) as part of this project?
- Please provide details of the sites you require access to, including the URLs
- Where are you planning to work from when you access these sites?
- Please provide details of how you are planning to capture/record the information you access on the sites listed, including any photos or other media, and how it will be stored
- Who will be using the materials accessed on the sites?
- Please outline how the data will be used in the research publication
- Expected start date for accessing the sites listed
- Expected end date for accessing the sites listed
- Please outline your data retention plan (how long will the data be kept, location, access management) and how you intend to remain compliant with regard to data protection regulations
- How are you planning to look after your wellbeing if the materials you access have a detrimental effect?
- Please outline your plan for ethics approval
- Please outline your plan for supervision