**Guidance on Access to Restricted Materials**

The process for recording access to restricted materials is to enable the University to identify where legitimate access is taking place and therefore, protect staff and students from potentially being investigated. The approval level will depend on the sensitivity of the materials being accessed and the wider remit of the research project. All requests submitted through this process will be reported to IGSSG and any other relevant groups.

For all access to restricted materials, individuals should ensure they have completed the online Information Governance training course and are aware of the risks. For example, access to the dark web also increases the risk of malware and viruses infecting information systems so users should ensure any unusual IT activity is reported immediately. Requestors should also ensure they are aware of other relevant policies and guidance such as the Safeguarding policy. Any concerns with information accessed should be reported (such as identifying criminal activity).

This document provides guidance on the level of approval, how to store and publish data and who we may be required to inform. Please note this is a guide only and each case may need reviewing individually. If you have any queries in relation to research data please contact the Research Data Manager (rdm@exeter.ac.uk) or the Research Ethics and Governance Team (<http://www.exeter.ac.uk/cgr/researchethics/>), otherwise, please email infosecurity@exeter.ac.uk.

**Access Level**

|  |  |  |
| --- | --- | --- |
| **Level** | **Detail** | **Approval** |
| 1 | Use of TOR browsing to access publicly available information. No sensitive information is downloaded or stored.  | Supervisor / line manager |
| 2 | Desk based research on publicly available information. No human participants, no personally identifiable information, no primary/secondary data analysis | Supervisor/line manager |
| 3 | Human participants, personally identifiable information, sensitive material accessible by standard routes e.g.: search engines, libraries, archives | Relevant Research Ethics Committee |
| 4 | Restricted/sensitive data only available by non-standard routes such as the dark web browsing (e.g. TOR) | Relevant Research Ethics Committee |

**Types of Information Accessed**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Level** | **Examples** | **Approval** | **Staff guidance for safeguarding** **sensitive materials** | **Students guidance for safeguarding** **sensitive materials** | **Guidance for publication** | **Other info** |
| 4 | Proscribed terrorist organisations or terrorist activity (for example researching the names of people linked to proscribed organisations; watching beheading videos) | Ethics committee | Ensure that you have a strong password set on your laptop and your university IT account that meets the current policy guidelines (min 10 characters). Go to as.exeter.ac.uk/it/account/changepassword/changepassword for further details.Open/unsecured W-Fi connections must not be used for researching sensitive materials. The University’s VPN access must be used.All electronic devices used to store sensitive materials should be secured when not in use, i.e. in a lockable container and access is controlled.Removable storage should also be encrypted with AES-128 as a minimum and also locked away when not in use.University supplied computer equipment must be encrypted with BitLocker or VeraCrypt technology and patched with the latest security updates.Sensitive materials must not be emailed outside of the University estate without applying encryption. Encryption could include applying passwords, but passwords must not be shared by email.Sensitive materials should not be stored on personal devices or emailed to personal mailboxes. The use of N drives (shared network folders) to store sensitive materials is strictly prohibited.SharePoint must not be used to store sensitive materials or for collaboration purposes on sensitive research projects.University U drives (personal storage for staff) can be used to store research. Documents should be password protected.Paper documents to be securely locked up with controlled access and papers destroyed in a confidential waste bin.Videos, films and interviews should not be downloaded and stored for later use. Encryption credentials must be stored securely. The use of a password manager tool is permitted, providing the master password has at least 16 letters. The National Cyber Security Centre’s advice is to use a collection of random dictionary words.Please ensure that you clear sensitive data from any unencrypted areas at end of session, e.g. download or temporary files, that are not encryptedAny deviations to the controls above must be notified to the information-security@exeter.ac.uk mailbox. If you  | The list below provides examples of security controls for students undertaking research in sensitive materials. This list is not exhaustive, and should the nature of the material that you will be accessing require it, your notification request will be passed to the Information Security Team for further advice.Folder level encryption is adequate, however full disk encryption should be used where possible. For example BitLocker, VeraCrypt, FileVault or other industry approved technologies. PCs/laptops must be patched with the latest security updates.Open/unsecured W-Fi connections must not be used for researching sensitive materials. Either the University’s VPN access must be used or students can set up a secure mobile hotspot using their own devices.University U drives (personal storage for staff) must be used to store research. This ensures your research is backed up. Research documents must be password protected.The use of N drives (shared network folders) to store sensitive materials is strictly prohibited.Videos, films and interviews should not be downloaded and stored for later use. All electronic devices used to store sensitive materials should be secured when not in use, i.e. in a lockable container and access is controlled.Removable storage should also be encrypted with AES-128 as a minimum and also locked away when not in use.Paper documents to be securely locked up with controlled access and papers destroyed in a confidential waste bin.Ensure that you have a strong password set on your laptop and your university IT account that meets the current policy guidelines (min 10 characters). Go to as.exeter.ac.uk/it/account/changepassword/changepassword for further details.Encryption credentials must be stored securely. The use of a password manager tool is permitted, providing the master password has at least 16 letters. The National Cyber Security Centre’s advice is to use a collection of random dictionary words.The University can accept no responsibility for the loss of data or encryption keys.Please ensure that you clear sensitive data from any unencrypted areas at end of session, e.g. download or temporary files, that are not encryptedAny deviations should be reported to the SID sid@exeter.ac.uk or 0300 555 0444 (UK) | University of Exeter Open Access Research and Research Data Management Policy http://www.exeter.ac.uk/research/openresearch/policies/exeter/; publisher and authorship guidelines; any terms included in ethical review decision | Statistics reported internally to the University Prevent Compliance Group. No personal information is included within this report.  |
| 4 | Not publicly available – Materials in restricted collections/ archives or accessed via dark web browsing (e.g. TOR). Insurgent groups’ propaganda materials  | Ethics Committee | As above | As above | University of Exeter Open Access Research and Research Data Management Policy http://www.exeter.ac.uk/research/openresearch/policies/exeter/; publisher and authorship guidelines; terms of use agreed with owners of restricted collections/archives | Statistics reported internally to the University Prevent Compliance Group. No personal information is included within this report. |
| 2 or 3 | Publicly available materials – social media, Insurgent groups’ propaganda materials such as the Islamic State ‘Dabiq’ or ‘Enquire’ magazines accessed via normal search engines | 3 - Ethics Committee if combined with other factors such as human participant research2 – Supervisor or line manager | Follow research data management and information security guidance, may require restricting depending on source/content.  | Follow research data management and information security guidance, may require restricting depending on source/content.  | University of Exeter Open Access Research and Research Data Management Policy http://www.exeter.ac.uk/research/openresearch/policies/exeter/; publisher and authorship guidelines; | Statistics reported internally to the University Prevent Compliance Group. No personal information is included within this report. |
| 2 or 3 | * The sex trade (for example information relating to sex workers including accessing blocked websites)
* Pornography and/or sexual abuse
* Human trafficking or the smuggling of migrants
* Child abuse
* Drug research
* Other criminal activity
 | 3 – Ethics Committee if combined with other factors such as human participant research2 – Supervisor or line manager | Follow research data management and information security guidance, may require restricting depending on source/content. | Follow research data management and information security guidance, may require restricting depending on source/content. | University of Exeter Open Access Research and Research Data Management Policy http://www.exeter.ac.uk/research/openresearch/policies/exeter/; publisher and authorship guidelines; any terms included in ethical review decision | Awareness of safeguarding policy.Knowing where/how to report concerns |
| 1 | * Testing of IT systems from ‘outside the network’ using the dark web browsing (eg TOR)
* No downloading of information
 | Supervisor or line manager | N/A no data download | N/A | N/A | N/A |