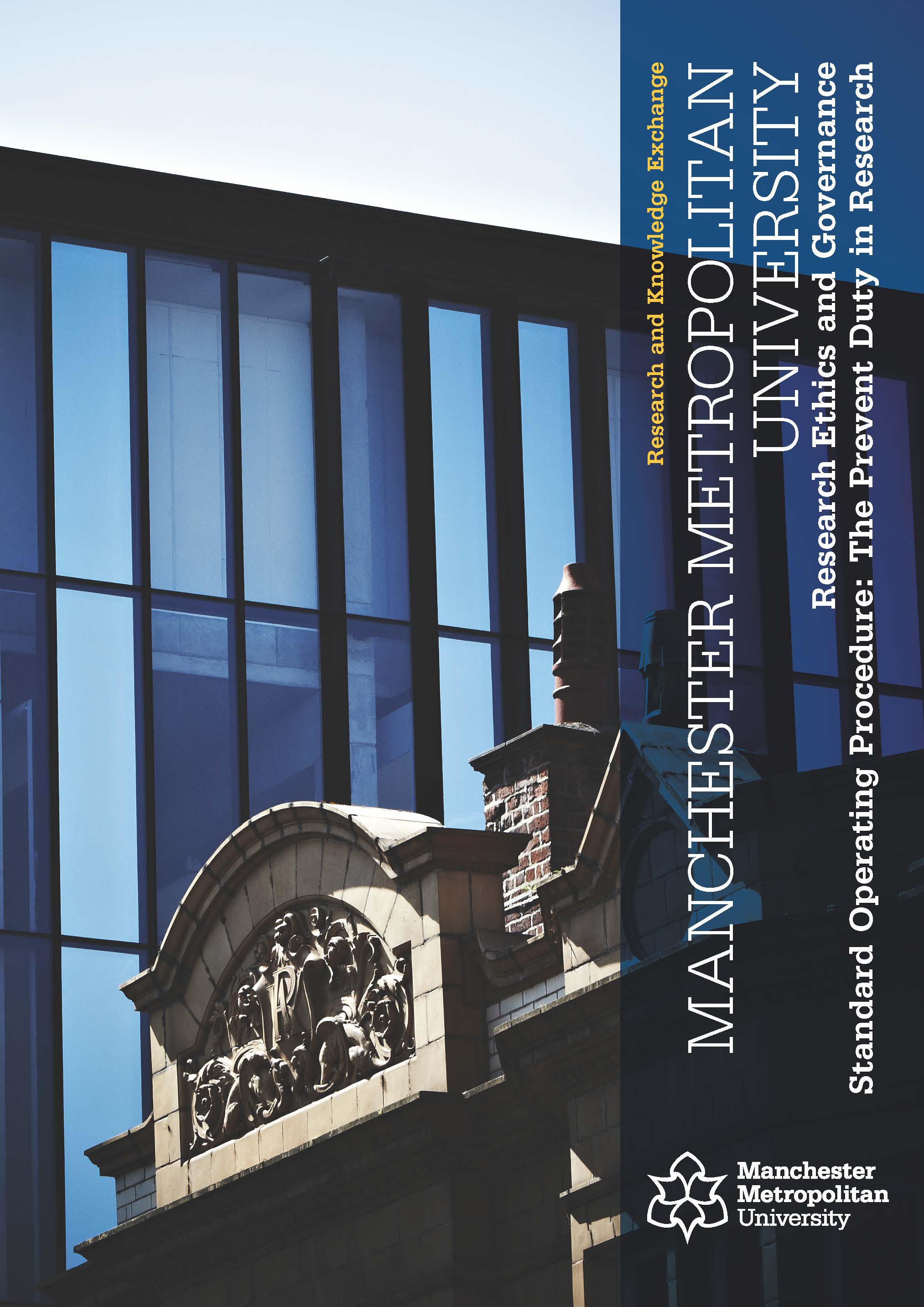
****

**PREVENT DUTY IN RESEARCH**

|  |  |
| --- | --- |
| Reference Number | MMU-RKE SOP 016 |
| Version | June 2019 |
| Effective Date | 05/06/2019 |
| Review Date | 01/07/2020 |
| Author | Ramona Statache, Research Ethics and Governance Manager |
| Approved by  Date | Prof Richard Greene, Pro-Vice-Chancellor Research and Knowledge Exchange  05/06/2019 |

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Reason for Change** |
|  |  |  |

This is a controlled document. The master document is posted on the RKE website:

http://www2.mmu.ac.uk/research/research-governance/

Any print-off of this document will be classed as uncontrolled. Researchers and their teams may print off this document for training and reference purposes but are responsible for regularly checking the RKE website for more recent versions.

1. **Introduction**

This Standard Operating Procedure (SOP) describes the process that Manchester Metropolitan University staff and students should follow in relation to the declaration and management of research and research data relating to terrorist-related activity related to the Prevent Duty. It is not the intention of this procedure to remove the obligations that staff and students have to comply with the University’s Academic Ethical Framework or to follow all of the usual process around insurance, health and safety and research governance more generally.

1. **Background**

The Counter-Terrorism and Security Act 2015 (‘the Act’) places a duty on ‘specified authorities’, including universities, to have ‘due regard to the need to prevent people from being drawn into terrorism’ in the exercise of their functions. In September 2015, the Government issued Prevent Duty Guidance under the Act, which included specific Guidance for higher education providers. The full Guidance can be found at: <https://www.gov.uk/government/publications/prevent-duty-guidance>.

1. **Purpose**

This Standard Operating Procedure (SOP) establishes best practice recommended for staff and students to enable them to meet their obligations under the Prevent Duty in research. Terrorism focus in research can be perceived by observers as actual terrorism and reported accordingly. Observers can be members of staff, students, members of the public, or representatives of various authorities. Activities that can raise suspicion include viewing, downloading, storing, reproducing, discussing or displaying any terrorism-related information or materials. To avoid situations where research into terrorism is reported to the authorities as actual terrorism, the University implements the following procedure.

1. **Procedure** 
   1. **Declaring terrorism-related academic interest**

The researcher is responsible for registering their terrorism-related interest with the Research Ethics and Governance Manager (REGM) by submitting the Prevent Duty in Research Form (Appendix 1). This form is usually submitted as part of the online application process for ethical approval for research using “EthOS, but the form can also be submitted to the REGM as a standalone item when academic terrorism-related interest is not associated with an active research project. Please note that the applicant’s declaration of terrorism-related academic interest must be confirmed by a line manager or Head of Department (in the case of staff) or an academic supervisor (in the case of students). The REGM reviews the application and indicates the appropriate action to be followed. Registration of terrorism-related academic interest with the REGM serves a dual purpose: appropriate facilities and processes can be put in place for the management of the data and confirmation of legitimate academic interest can be made by the University on behalf of the researcher.

* 1. **Virtual secure store “SharePoint”**

As part of the registration process of terrorism-related academic interest, the REGM allocates a secure virtual folder in SharePoint to the applicant. User access to SharePoint can be managed at a folder level, and administration of user access is assigned to the REGM and an Information Security Manager (ISM), who have view of the store’s list of file names but cannot access the contents of the files. Any change to store access requires written approval from the REGM, who also notifies the ISM. Contact details for both the REGM and the ISM are provided below. Maintenance of the “SharePoint” solution resides with the Director of ISDS.

* 1. **Managing terrorism-related research data**

When the Prevent Duty in Research Form is submitted on behalf of a research project, a folder is allocated to the Principal Investigator (PI) in SharePoint. The PI has a duty to inform the REGM of the identity of all the project team members who are given access to it. When the Form is submitted as a standalone application, the SharePoint folder is allocated solely for the benefit of the applicant.

The approved users MUST:

* keep all electronic terrorism-related materials in the SharePoint folder that is assigned by the REGM;
* scan all paper terrorism-related material, upload it to the SharePoint folder, and dispose of the paper versions;
* access terrorism-related websites from the University IT network using a University approved device.

The approved users MUST NOT allow terrorism-related materials to be:

* stored or processed on any non-approved devices, whether personal or University issued;
* stored on removable data storage devices (e.g. USB memory sticks, hard drives) or commercial storage space (e.g. cloud storage, personal Dropbox);
* uploaded to shared drives other than SharePoint (e.g. the University’s Staff to Staff (R drive), Staff to Student (S drive) or Home (H drive).
* transmitted via email or any other channel of dissemination, electronic or paper-based;
* held in physical format.

Whilst a researcher is using a document from the SharePoint folder, they must not leave their computer unattended.

* 1. **Persons observing suspicious activities or events**

Members of staff and students who think they might have observed a suspect event are advised to follow the University procedure outlined in the University’s Prevent Duty Staff Briefing Note, section ‘4i Concerns about students or members of staff’. The latest version of the Briefing Note is on the Staff Intranet at:

<https://mmuintranet.mmu.ac.uk/Interact/Pages/Content/Document.aspx?id=3062>

It is acknowledged that staff whose work may fall within the remit of the Prevent agenda are more likely to come across situations or material that may cause them concern in relation to public safety or potential terrorist-related activity. In these situations, staff should contact the Head of Facilities Management Programmes and Campus Security (extension 1386) in the first instance. If a staff member carrying out Prevent related research feels that some sort of terrorist incident is imminent then they should, of course, contact the Police immediately.

Upon receipt of an internally reported concern or of an enquiry from external agencies, the members of staff designated above should contact the REGM to verify if the person in question is registered with the University as having a legitimate terrorism-related academic interest.

The REGM to be contacted is:

Ramona Statache, Research Ethics and Governance Manager, RKE Directorate([r.statache@mmu.ac.uk](mailto:r.statache@mmu.ac.uk); ext. 2853).

In her absence, confirmation of registration should be sought from:

Alison Lloyd, Research Ethics and Governance Manager, RKE Directorate, ([a.lloyd@mmu.ac.uk](mailto:a.lloyd@mmu.ac.uk), ext. 2836)

Tom Stoddart, Assistant Director Information Security, ([t.stoddart@mmu.ac.uk](mailto:t.stoddart@mmu.ac.uk); ext. 6755).

1. **Related Documents**

Prevent Duty in Research Form (Appendix 1)

**APPENDIX 1**

**Prevent Duty in Research Form**

As described in SOP16 (<http://www2.mmu.ac.uk/research/research-governance/>), the University has a legally mandated Prevent Duty regarding terrorism. If your research potentially involves this topic, please notify the Research Ethics and Governance Manager (REGM) by returning this form to [ethics@mmu.ac.uk](mailto:ethics@mmu.ac.uk). Researchers who are submitting an application through EthOS for ethical approval do not need to engage with the Prevent Duty Form as this is included in the EthOS form.

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Title** |  | | |
| **Ethics application reference number** |  | | |
| **Start / end date of project** |  | | |
| **Name of applicant** |  | | |
| **Role of applicant in project** |  | | |
| **Status of applicant (Staff, PGR, PGT)** |  | | |
| **Faculty** |  | | |
| **School / Department / Unit** |  | | |
| **Programme of study**  **(if applicable)** |  | | |
| **Name of supervisor or**  **line manager** |  | | |
| **Co-workers in the project**  **with access to the declared**  **materials (name, MMU ID,**  **project role)** |  | | |
|  | | |
|  | | |
|  | | |
| **Project Description** (No more than 1 page. Please refer to: background, research question/aim, methodology, method, planned activities, risks and risk mitigation. Add any other details you consider relevant.) | | | |
|  | | **Mark the appropriate box with an X** | |
|  | | **YES** | **NO** |
| 1. Does your research include activities or materials related to terrorism? | |  |  |
| 1. If you answered ‘Yes’ to question 1, you are required to digitise all relevant material and store it in a secure university file store that the REGM will allocate to you. Access to this store will be authorised only for the persons you nominated above.   Do you agree to keep all relevant documents in the provided secure file store? | |  |  |
| 1. Do you need to access these stored materials from outside the University’s IT network? | |  |  |
| 1. If you answered ‘Yes’ to question 3, please indicate that you understand that access to the secure file store will only be possible via the University’s SSL VPN solution. | |  |  |
| 1. Do you agree to abide fully by the data management requirements listed in section 4.3 of the University’s SOP16? | |  |  |
| 1. Will your research involve visits to websites that might be associated with extreme, terrorist, or criminal organisations / activities? | |  |  |
| 1. If you answer ‘Yes’ to question 6, you are advised that such sites may be subject to surveillance by the police. Accessing those sites from home or university IP addresses might lead to police enquiries. Please indicate that you understand this. | |  |  |
| 1. By submitting to the MMU ethics process, you accept that authorised members of the University’s central ethics and IT teams will have access to a list of file names (but not file contents) in your secure store. | |  |  |

|  |  |
| --- | --- |
| **Signed by applicant:** | **Date:** |
| **Name** (in print) | |

|  |  |
| --- | --- |
| **Countersigned by supervisor / manager / head of department:** | **Date:** |
| **Name** (in print) | |

Please return this form to:

Ramona Statache

Research Ethics and Governance Manager

G12 Ormond Building

Lower Ormond Street

Manchester

M15 6BX

[ethics@mmu.ac.uk](mailto:ethics@mmu.ac.uk)