# Plan Overview

*A Data Management Plan created using DMPonline*

**Title:** APP8020: SALIENT: Building a Secure And ResiLIENT World: Research and Coordination Hub

**Creator:** First Name Surname

**Principal Investigator:** Richard Kirkham

**Project Administrator:** Victoria Turner, Darren Clement

**Affiliation:** University of Manchester

**Funder:** UKRI Future Leaders Fellowships

**Template:** UKRI Future Leaders Fellowships Template for a Data Management Plan Customised By: University of Manchester

**Project abstract:**

Building a Secure and Resilient World (BSRW) will take a systemic approach that is human-centred, aimed at strengthening societal and economic resilience, and enhancing security across virtual and physical environments, by improving awareness of risks and threats, preparedness, informed decision-making and response. It will work towards change being understood as a force for good.

The Research and Coordination Hub is a significant opportunity to shape this theme and make a major and lasting contribution to developing the UK's resilience and security framework.

The hub will coordinate and maximise the impact of the range of activities commissioned by UKRI ensuring an integrated approach throughout. It will be expected to lead, plan, deliver and manage a multidisciplinary programme of research and devolved funding opportunities in identified areas of knowledge and evidence gaps within the scope of the theme outlined above.

This will require the hub to build strong connections with a variety of stakeholders across central and local government, devolved administrations, internationally and the general public. These devolved awards will generate a rich and diverse portfolio of interdisciplinary research and innovation that directly engages with the priorities and subthemes of the BSRW programme:

- global order in a time of change
- technologies for resilience, security and defence
- resilient and secure supply chains
- behavioural and cultural resilience
- strengthening resilience in natural and built environments

**ID:** 128023

**Start date:** 01-02-2024

**End date:** 31-01-2029

**Last modified:** 17-07-2023

**Grant number / URL:** https://www.ukri.org/opportunity/building-a-secure-and-resilient-world-research-and-coordination-hub/

**Copyright information:**

## APP8020: SALIENT: Building a Secure And ResiLIENT World: Research and Coordination Hub

**Manchester Data Management Outline**

**1. Will this project be reviewed by any of the following bodies (please select all that apply)?**

- Funder

**2. Is The University of Manchester collaborating with other institutions on this project?**

- Yes - Part of a collaboration and owning or handling data

The University of Manchester will co-ordinate the proposed hub (SALIENT) including the allocation of devolved funding and the subsequent project management and assurance. Therefore, data which is required for the good governance of the hub, will be held by the Thomas Ashton Institute (TAI) and may be shared with collaborating institutions where required. It is plausible to foresee some DF awards to researchers at The University of Manchester; in these cases the PI will be required to adhere to the institutional polices identified in Section 7 of this DMP.

**3. What data will you use in this project (please select all that apply)?**

- Acquire new data

**4. Where will the data be stored and backed-up during the project lifetime?**

- University of Manchester Research Data Storage Service (Isilon)

**5. If you will be using Research Data Storage, how much storage will you require?**

- < 1 TB

**6. Are you going to be receiving data from, or sharing data with an external third party?**

- Yes

The SALIENT hub will receive external third party data as part of the 'business as usual' aspects of co-ordination. The DF PI's may require data sharing agreements depending upon the nature of their research; in these cases,

**7. How long do you intend to keep your data for after the end of your project (in years)?**

- 0-4 years

*Guidance for questions 8 to 13*
**Highly restricted information defined in the [Information security classification, ownership and secure information handling SOP](#) is information that requires enhanced security as unauthorised disclosure could cause significant harm to individuals or to the University and its ambitions in respect of its purpose, vision and values. This could be: information that is subject to export controls; valuable intellectual property; security sensitive material or research in key industrial fields at particular risk of being targeted by foreign states. See more [examples of highly restricted information](#).**

**If you are using 'Very Sensitive' information as defined by the [Information Security Classification, Ownerships and Secure Information Handling SOP](#), please consult the [Information Governance Office](#) for guidance.**
**Personal information, also known as personal data, relates to identifiable living individuals. Personal data is classed as special category personal data if it includes any of the following types of information about an identifiable living individual: racial or ethnic origin; political opinions; religious or similar philosophical beliefs; trade union membership; genetic data; biometric data; health data; sexual life; sexual orientation.**
**Please note that in line with [data protection law](#) (the UK General Data Protection Regulation and Data Protection Act 2018), personal information should only be stored in an identifiable form for as long as is necessary for the project; it should be pseudonymised (partially de-identified) and/or anonymised (completely de—identified) as soon as practically possible. You must obtain the appropriate [ethical approval](#) in order to use identifiable personal data.**

**8. What type of information will you be processing (please select all that apply)?**

- Personal information, including signed consent forms

**9. How do you plan to store, protect and ensure confidentiality of any highly restricted data or personal data (please select all that apply)?**

- Store data on University of Manchester approved and securely backed up servers or computers
- Where needed, follow University of Manchester guidelines for disposing of personal data
- Impose suitable non-disclosure agreements (e.g. for managers or users of personal data)
- Impose suitable data sharing and collaboration agreements

**10. If you are storing personal information (including contact details) will you need to keep it beyond the end of the project?**

- Yes – Funder requirement

**11. Will the participants' information (personal and/or sensitive) be shared with or accessed by anyone outside of the University of Manchester?**

- Yes - Public institutions with contractual arrangements (e.g. NHS research sites or other higher education institutions)

The hub will share personal information with collaborating institutions where appropriate

**12. If you will be sharing personal information outside of the University of Manchester will the individual or organisation you are sharing with be outside the EEA?**

- No

**13. Are you planning to use the personal information for future purposes such as research?**

- No

**14. Will this project use innovative technologies to collect or process data?**

- No

**15. Who will act as the data custodian for this study, and so be responsible for the information involved?**

Dr Richard Kirkham

**16. Please provide the date on which this plan was last reviewed (dd/mm/yyyy).**

2023-07-12

**0. Proposal name**

**0. Enter the proposal name**

SALIENT: Building a Secure And ResiLIENT World: Research and Coordination Hub

**1. Description of the data**

**1.1 Type of study**

SALIENT is comprised of two components; a co-ordination hub and a devolved funding (DF) programme. At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point. The coordination hub will gather data on the nature of the studies undertaken within the DF element, primarily for the purposes of project management and assurance. The hub will not hold research data associated with the DF element.

**1.2 Types of data**

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be

specified at this point.

### 1.3 Format and scale of the data

Coordination hub data will be collected and maintained on a database housed within the University of Manchester's IT infrastructure. At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature, format and scale of the data that is to be collected cannot be specified at this point.

## 2. Data collection / generation

### 2.1 Methodologies for data collection / generation

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point. Personal data collected by the hub for the purposes of project management and assurance will be held in accordance with the policies described in Section 7 of the DMP.

### 2.2 Data quality and standards

It is likely that we will seek to capture audio, video or images of participants at events taking place during the lifecycle of SALIENT, we will adhere to the guidance described in Taking recordings of participants for research projects SOP as this data must be processed in accordance with data protection laws.
In terms of the DF element of SALIENT, we are unable to state how consistency and quality of data collection / generation will be controlled and documented, be this through processes of calibration, repeat samples or measurements, standardised data capture or recording, data entry validation, peer review of data or representation with controlled vocabularies.

## 3. Data management, documentation and curation

### 3.1 Managing, storing and curating data

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point. Personal data collected by the hub for the purposes of project management and assurance will be held in accordance with the policies described in Section 7 of the DMP.

### 3.2 Metadata standards and data documentation

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point. We recognise that using community metadata standards improves the discoverability of data produced within the DF portfolio and facilitates combination of data sets.

### 3.3 Data preservation strategy and standards

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point. Personal data collected by the hub for the purposes of project management and assurance will be held in accordance with the policies described in Section 7 of the DMP.

## 4. Data security and confidentiality of potentially disclosive information

### 4.1 Formal information/data security standards

The University of of Manchester's information and data policies are identified in Section 7 of this Data Management Plan.

### 4.2 Main risks to data security

The SALIENT hub will collect and store data in relation to project management and assurance. We will not collect or store data associated with devolved funding projects which may are approved and funded by the hub; this will be the responsibility of the individual PI's and their respective institutions. To ensure SALIENT is compliant with existing information and data security standards, we will ensure:

1. Full system encryption is performed by default on all new laptops by IT Services staff as part of the setup and installation process, before delivery to the end user. Full system encryption of existing desktop and laptop computers is strongly recommended when sensitive data is stored locally and can be requested via the University's IT Service Desk (see the contact list section for details).

2. That desktops and laptops are secured with anti-theft devices to provide additional physical IT Security.

3. The SALIENT hub core team do not share sensitive data by email. Where this is unavoidable the data must be anonymised, with the key index sent separately. If sensitive data must be sent via email then the sensitive data should be encrypted using University prescribed encryption software prior to sending to an authorised party. A strong, complex passphrase should be used to encrypt the data and this passphrase should only be relayed to the recipient via an alternative method of

communication, such as telephone or text message, once the identity of the recipient has been confirmed.

The University of Manchester's IT Security Policies (see Section 7) arwe based on UCISA best practice, which, in turn, draws heavily on the standards BS7799 and ISO 27001.

In June 2023, The University of Manchester experienced a cyber attack; the incident is live as of the date when this DMP was produced. Based on UoM investigations to date, IT services believe that a small proportion of data has been copied by a criminal entity that relates to some students, and some alumni. The University has written directly to those individuals who may have been affected by this.

## 5. Data sharing and access

### 5.1 Suitability for sharing

The answers provided in this section relate to the devolved funding (DF) element of the SALIENT Hub and therefore are relevant to any research projects that are are approved and funded by the Hub during the life-cycle of SALIENT. The coordination hub will gather data on the nature of the studies undertaken within the DF element, primarily for the purposes of project management and assurance. The hub will not hold research data associated with the DF element.

At the moment, it is not known what studies will be undertaken as part of the DF element, and therefore, the nature of the data that is to be collected cannot be specified at this point.

### 5.2 Discovery by potential users of the research/innovation data

It is for individual research participants (and their organisations) to decide if, and how, data generated from DF projects is made available. Through the SALIENT hub, we will promote the University of Manchester's policies on 'Open Research'; specifically

We will seek evidence, in the appraisal of DF applications, of actions to support 'Research transparency', which encompasses a range of open practices including registering studies, sharing study data, and publicly reporting research findings. SALIENT researchers will be encouraged to adopt transparent and responsible practices to improve research integrity and the trustworthiness of scientific findings generated from their studies.

We will encourage 'registration of research methodology' and intended analyses as this increases researcher accountability and improves credibility. SALIENT recognises that sharing of additional research outcomes such as study data, reproducible scripts, software, and protocols allows for both replication and extension of the work by others.

We will encourage the open dissemination and reporting of outcomes, this improves access to scientific knowledge, allowing policy makers and the public to use research findings to make informed decisions.

SALIENT will state our policy and approach to data sharing on the SALIENT website (or by other means).

### 5.3 Governance of access

The PI will be responsible for making the decision on whether to supply SALIENT hub data to a potential new user. For DF projects, it will be the responsibility of the PI at the relevant institution. It is not yet possible to determine whether the data will be deposited in and available from an identified community database, repository, archive or other infrastructure established to curate and share data.

### 5.4 The study team's exclusive use of the data

SALIENT recognises UKRI's requirement is for timely data sharing, with the understanding that a limited, defined period of exclusive use of data for primary research/innovation is reasonable according to the nature and value of the data, and that this restriction on sharing should be based on simple, clear principles. The SALIENT hub will operate in ways that are consistent with the University of Manchester's 'Open Research' policies and promote the spirit of Open Research throughout the life-cycle of the hub. It will be the responsibility of PI's in receipt of DF to determine their own approach, ensuring that this aligns with institutional governance requirements and is consistent with the aspirations of SALIENT.

### 5.5 Restrictions or delays to sharing, with planned actions to limit such restrictions

The nature of information sharing agreements with (say) Government Departments may require a restriction to data sharing - this is more likely to arise in the context of DF projects where access to data is pre-requisite on a confidentiality agreement (CA) or non-disclosure agreement (NDA). The Thomas Ashton Institute (TAI) has significant experience in preparing agreements of this nature and will offer counsel to DF researchers as appropriate.

Clearly, it is the responsibility of DF PI's to determine the most appropriate strategies to limit restrictions on data sharing (where required by an CA or NDA) which may include data being anonymised or aggregated; gaining participant consent for data sharing; gaining copyright permissions.

For prospective studies that may occur within SALIENT, consent procedures should include provision for data sharing to maximise the value of the data for wider research/innovation use, while providing adequate safeguards for participants. As part of the consent process, proposed procedures for data sharing should be set out clearly by PI's and current and potential future risks associated with this explained to participants.

### 5.6 Regulation of responsibilities of users

It is likely that PIs will have to consider if external users of data will be required to sign and abide by data sharing agreements. It may be that bespoke individual agreements will be required - these are decisions that potential PI's will be expected to demonstrate awareness of in their submissions to the DF funding pool.

## 6. Responsibilities

### 6. Responsibilities

The PI will be responsible and accountable for data management, metadata creation, data security and quality assurance of data in relation to management and co-

ordination of the SALIENT hub. The Thomas Ashton Institute manages data in accordance with the University of Manchester's policies which are identified in Sct. 7 of this Data Management Plan.

In the Devolved Funding element of SALIENT; awardees (as PI's) will be responsible for data management in relation to their projects; it is expected that DF PI's will adhere to their own institutional policies and procedures.

## 7. Relevant policies

**7. Relevant institutional, departmental or study policies on data sharing and data security**

| Policy | URL or Reference |
|---|---|
| Data Management Policy & Procedures | https://documents.manchester.ac.uk/display.aspx?DocID=33802#:~:text=Research%20data%20is%20to%20be%20stored%2C%20made%20available%20and%20assigned,or%20contractual%20rights%2 |
| Data Security Policy | https://documents.manchester.ac.uk/display.aspx?DocID=6525#:~:text=Confidentiality%20%2D%20information%20is%20protected%20from,integrity%20of%20externally%20provided%20data |
| Data Sharing Policy | https://www.library.manchester.ac.uk/services/research/research-data-management/sharing/ |
| Institutional Information Policy | https://www.library.manchester.ac.uk/services/research/research-data-management/sharing/ |

## 8. Author and contact details

**8. Author of this Data Management Plan (Name) and, if different to that of the Principal Investigator, their telephone & email contact details**

Not applicable

.