DATA MANAGEMENT PLAN

## 0. Proposal name

Role of senescent keratinocytes and fibroblasts in cutaneous inflammation

## 1. Description of the data

### 1.1 Type of study

Cross-sectional study using human tissue samples for analysis and in vitro functional studies using human cells

### 1.2 Types of data

We will generate single cell datasets (scRNA-seq and scATAC-seq) and detailed histological images of tissue. We will measure routine clinical parameters and obtain data from medical records at Sandwell and West Birmingham NHS Trust. Laboratory data will include images, flow cytometry datasets and quantitative cytokine profiles (stored as electronic numerical values) and hand-written laboratory notebooks and printed reports.

### 1.3 Format and scale of the data

Most data including laboratory and clinical data will be in numerical format (with some string variables) and stored in standard file types (e.g. .csv) for downstream analysis in standard packages (Graphpad Prism, STATA, R). Images will be stored as .tiff or .qptiff files and analysed in QuPath and R. Single cell data will be stored as .bam and .fastqz files. After downstream analysis they will be stored as R dataframes. Single-cell data are typically around 1.5GB in size, and we anticipate a total size of 72GB for both scRNA-seq and scATAC-se data.

## 2. Data collection / generation

### 2.1 Methodologies for data collection / generation

Data will be generated from the laboratory experiments and analysis of human tissue (both sequencing of dissociated cells and images of tissue sections). All data processing steps will be logged in scripts to ensure transparency and reproducibility. Laboratory experiments will be clearly documented in laboratory notebooks.

### 2.2 Data quality and standards

Laboratory experiments will follow established protocols or SOP. Participant study visits will follow an established SOP. Single cell analysis and tissue analysis will be conducted in conjunction with Genomics Birmingham and Birmingham Tissue Analytics respectively which will ensure high standards of data quality according to Good Laboratory Practice. All data will be rigorously reviewed to ensure that it is high quality and reproducible and experiments will be repeated as described in the Case for Support and Annex.

## 3. Data management, documentation and curation

### 3.1 Managing, storing and curating data.

Prior to publication, all data files will be stored within individual directories on secured hard drives on encrypted computers at the University of Birmingham. Data from team members will be shared via Microsoft 365 applications OneDrive and MS Teams provided by the University of Birmingham. No personal identifiable data will be stored on UoB servers. All data will be secured and backed-up on the University of Birmingham servers according to the University’s data management policies (see below).

### 3.2 Metadata standards and data documentation

Detailed metadata for the samples will be stored along with a data dictionary where necessary. Handwritten laboratory books will be used to document each of the experiments. All protocols will be stored in a central repository to ensure consistency in the conduct of experiments.

### 3.3 Data preservation strategy and standards

All essential documentation will be archived in accordance to applicable regulatory requirements. Data, including consent forms, clinical data, single-cell datasets, images and laboratory data, will be archived for at least 10 years following study completion on secure servers (BEAR Archive at UoB) which are regularly backed up and managed by the University of Birmingham’s IT department. Following this period, paper copies of consent forms will be securely destroyed. Any datasets that might be valuable for further study will be fully anonymised.

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

### 4.1 Formal information/data security standards

The University of Birmingham maintains an Information Security Policy which has been specifically designed to be compliant with the ISO 27001/2 standards, and references the existing ‘Conditions of Use of Computing and Network Facilities’ and new ‘Codes of Practice’ encompassing use of computers, data use and security. These policies have been approved by Council, the University’s governing body, and are gradually being implemented across the whole university. Project team members will be trained in data security and confidentiality and support provided to enable action where necessary.

### 4.2 Main risks to data security

Personal data (e.g. on consent forms and link files will be stored at the NHS Trust according to local protocols. No personally identifiable data will be stored or analysed at UoB. Metadata about participants will be pseudo-anonymised and the link file held at the NHS Trust. In all cas-es, data will be stored on secure servers and if needed transferred using secure systems. No data will be transferred to personal devices as per the University of Birmingham’s Information Security policy.

## 5. Data sharing and access

### 5.1 Suitability for sharing

Anonymised single cell datasets will be shared using at Gene Expression Omnibus (GEO) along with limited metadata (to ensure that anonymisation is maintained). Requests for additional data will be welcomed and given full consideration on an individual basis. No sharing will take place if confidentiality cannot be maintained.

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

Following completion of the study and publication of the manuscripts, the -omics data will be made available on online at Gene Expression Omnibus (GEO) and our analysis code will be deposited on GitHub. The study description and metadata catalogue will be made available via the MRC Research Data Gatrway.

### 5.3 Governance of access

Decisions about data access will be the responsibility of the PI. As it is anticipated that requests will occur on an occasional basis an independent advisor will review access request decisions post hoc. Any difficult decisions regarding data access will be deferred to the independent advisor in the first instance.

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

We will publish the findings of the research, in the format of a peer-reviewed manuscript as soon as possible. Data will be embargoes until data is published in complete form after which we will make the -omics datasets freely available.

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

We don’t foresee and restrictions other than retaining the right to exclusive use of the data until publication is complete as outlined above. As described above, some data may be redacted if it would allow individual participants to be identified.

### 5.6 Regulation of responsibilities of users

The research team will agree not to transfer data to another unauthorised third-party. Access to study data by external users will be bound a data sharing agreement, which will specify conformance to the MRC data sharing guidance. The agreement will address handling of intellectual property, publication, authorship, acknowledgement and whether data are provided on an “exclusive” or “non-exclusive” basis to the requester. It will include that the output based on the data are reported to the owners of the data and that MRC be acknowledged in outputs

## 6. Responsibilities

All grant holders and employed staff will be responsible for study-wide data generation, management, quality assurance and data security. University of Birmingham has mandatory information security and data management training courses to be completed by all staff mem-bers every two years. The Information Technology Support team will take responsibility for data security, storage, back-up and access.

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

### Policy URL or Reference

#### Data Management Policy & Procedures

University Data Management Policy:

<http://www.birmingham.ac.uk/Documents/university/legal/data-prot-policy.pdf>

University Code of Practice for Research:

<http://www.birmingham.ac.uk/Documents/university/legal/research.pdf>

Record Management Guidelines:

<https://intranet.birmingham.ac.uk/as/libraryservices/records/guidelines.aspx>

General Medical Council’s Principles of Good Research Practice:

<http://www.gmc-uk.org/guidance/ethical_guidance/6001.asp>

Data Security Policy

IT policies on data sharing and security:

<http://www.it.bham.ac.uk/policy>

Data Sharing Policy

IT policies on data sharing and security:

<https://intranet.birmingham.ac.uk/as/libraryservices/library/research/rdm/archiving-data/archiving-and-sharing-data.aspx>

Institutional Information Policy

University Code of Practice for Research:

<http://www.birmingham.ac.uk/Documents/university/legal/research.pdf>

Record Management Guidelines:

<https://intranet.birmingham.ac.uk/as/libraryservices/records/guidelines.aspx>

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

XXXXXXXXXXXXX