Research Governance Office Sponsorship Standard Operating Procedures

Data Governance

SOP Reference	S-1036
Version and Date	V4.0 April 2026
Author	
Name	Claire Fitzpatrick
Job Title	Research Quality Assurance Officer
Name	Kyla Harrington
Job Title	Clinical Trials Governance Manager
Reviewer/Approver	
Name	Dr Cat Taylor
Job Title	Head of Research Governance
Signature	
Date	28 April 2026
Effective Date*	28 April 2026
Next Review Date	April 2029

1.0 Introduction and Scope

This Standard Operating Procedure (SOP) outlines the minimum standards for the management of research data throughout its lifecycle. It ensures that data collected, stored, analysed, and shared is handled in a way that protects participant rights and ensures the reliability of results.

This SOP applies to all research (referred to as 'trials' hereafter) sponsored by the University of Leicester (UoL).

2.0 Purpose

The primary objective is to maintain data integrity, traceability, and security.

Proportionality Statement: In accordance with ICH GCP E6(R3) and the UK Clinical Trials Regulations, the intensity of data management activities (e.g., validation, monitoring) must be proportionate to the risks to participant safety and the reliability of trial results.

This SOP has been authored in accordance with ICH GCP E6(R3) and the UK Clinical Trials Regulations 2025. While this document provides the University's minimum standards, investigators and research staff must refer to these primary regulatory sources to fully understand their legal and ethical responsibilities regarding data integrity and participant safety.

3.0 Responsibilities

- Chief Investigator (CI): Acts as the primary data custodian. Responsible for overall data security, regulatory compliance, and reproducibility of findings.
- Principal Investigator (PI): Responsible for the integrity and accuracy of data generated at their specific location.
- Sponsor (UoL): Responsible for institutional oversight of the integrity and confidentiality of data generated, and ensuring this SOP is implemented effectively.

4.0 Data Integrity: ALOCA+ Principles

An essential element of conducting research studies is efficient management of data integrity, traceability and security, thereby allowing the accurate reporting, verification and interpretation of research-related information. The quality and amount of information generated in a trial should be sufficient to address the objectives, provide confidence in the results and support good decision making. Only data that is essential for the purpose of the research and is as stated in the approved protocol should be collected.

All data must adhere to the ALCOA+ principles to ensure it is fit for purpose and is regulatory compliant.

Principle	Operational Definition
Attributable	Clearly linked to the individual who generated it and when (i.e., time/date stamped)

Legible	Easy to understand, readable and permanent
Contemporaneous	Recorded at the time the activity or observation occurs
Original	Preserved in its original form or a certified* copy
Accurate	A truthful representation of the observation, free from error
Plus (+)	• **Complete** – all required data must be recorded, including any corrections or amendments. • **Consistent** – data must follow a logical sequence and be recorded in accordance with the protocol and SOPs. • **Enduring** – maintained in a durable format for the required retention period. • **Available** – readily accessible for review, monitoring, audit, or inspection.

*The process for creating certified copies of source data is described SOP S-1015.

5.0 Source Records

Source records refers to the **original documents or data (which includes relevant metadata) or certified copies*, irrespective of the media used** that is collected during a trial that supports the findings and allows for verification, reconstruction, and evaluation of the research.

Source records must be:

- Securely stored in accordance with institutional policies and applicable data protection regulations (e.g., General Data Protection Regulation (GDPR));
- Retained and accessible for the duration of a trial (including its archive period); and
- Altered in a GCP compliant manner
  - For paper records this involves a single strikethrough so the original entry remains visible, the correction should be initialled and dated by the person making the change.
  - For electronic records there must be an audit trail, documenting what changes were made, by who and when).

Careful consideration must be given to the storage and retention of all formats of source records (especially perishable records and electronic data, including all metadata) and a sticker (or equivalent in electronic records) must be placed on the cover of the medical records indicating the ‘do not destroy before’ date.

5.1 Paper

Where paper CRFs and workbooks are being used, the following applies:

- Ensure the documents are version controlled and the correct versions are being used;
- Do not use materials such as sticky notes/scrap paper;
- Use a black pen with permanent, archival-quality ink (erasable pens, fountain pens, markers/highlighters and pencil must not be used);
- Sign and date all entries;

- Boxes **should not be** left blank/empty (the box should either have the data value or be annotated with UKN (unknown), ND (not done), NA (not applicable)); and
- Altered in a GCP compliant manner (explained above).

5.2 Electronic

- When data captured on paper or in an electronic format are then manually transcribed into a computerised system (e.g., data acquisition tool), the need for and the extent of data verification should take the criticality of the data into account;
- Where data verification is conducted, the initial transcription/entry should be followed by a second review, ideally by a different person, to identify errors;
- Standardise the use of medical terminology and formatting to produce consistency across entries;
- Acquired data from any source, including data directly captured in a computerised system (e.g., data acquisition tool), should be accompanied by relevant metadata;
- Regularly review for missing, inconsistent or out-of-range data; and
- Carefully manage CRF updates/modification implementation with change control and documentation of all modifications made (this is especially critical where the database mirrors the CRF and where modifications are made to the research that impact data collection and management).

5.3 Audio

- Where audio recordings are the source data, the following applies:
- Use high-quality encrypted recording equipment (personal devices must not be used);
- Choose quiet environments;
- Test before recording;
- Consider an SOP covering device set-up, file naming, storage and destruction;
- Store files in encrypted, access-controlled systems/locations (unsecured platforms must not be used);
- Consider double-transcription or using a University of Leicester-approved transcription service and check for accuracy; and
- Destroy audio files once transcription has been performed (unless approval has been received to retain).

6.0 Data Management Plan (DMP)

A DMP refers to the formal processes outlining how data will be collected, where it will be stored, how it will be protected, and whether and with who it will be shared. Careful consideration must be given to the format data is collected in, and the format of the output, to enable appropriate statistical analyses. Quality control (QC) must be applied at each stage of data handling to ensure that all data are accurate, reliable and have been processed correctly.

The type of DMP required depends on the type of trial:

- For Clinical Trials of an Investigational Medicinal Products (CTIMPs) and Medical Device Trials, the UKRI DMP template should be used unless the task of Data Management has been formally delegated to a third party (e.g., a CTU, CRO, or vendor) and the third party DMP template is being used.
- For all other research, the DMP process should be detailed within the protocol. The UKRI DMP template can be used if desired.

The DMP should:

- Be developed during the early stages of preparing the research;
- Be finalised before recruitment;
- Be adhered to throughout the lifecycle (where deviations occur, these must be documented);
- Be reviewed and updated (if applicable) periodically*, and following key time points such as CRF/database sign-off, modifications (especially where data management is impacted by a modification), database lock etc. and as necessary to reflect changes in trial procedures, data systems, or regulatory requirements.
- Detail the location of all datasets, including those external to the main trial database and should provide detail on how external data will be captured, transferred and reconciled.

*For CTIMPs and Medical Device Trials, in the absence of any other key time points, we recommend reviewing at the same time as completing annual reporting (i.e., Development Safety Update Report (DSUR)).

7.0 Responsibilities for Selecting Appropriate Data Capture Systems

Researchers are responsible for ensuring that all research data are captured, stored, and managed within an appropriate, secure, and controlled data capture system. This responsibility includes:

- Ensuring the system provides adequate technical and organisational controls, such as access restrictions, audit trails, version control, encryption, and secure backup.
- For CTIMPs - Using only University of Leicester approved systems for research data capture and storage, unless explicit approval has been granted through the appropriate governance processes. Note that new services and systems may require a Cloud Service Assessment before being approved for use. You must ensure there is sufficient time in the trial set-up to allow for the assessment.
- Confirming that any external or third-party system has undergone the required data protection impact assessment (DPIA) and that appropriate contractual arrangements (e.g., Data Processing Agreements) are in place.
- Maintaining data integrity, confidentiality, and availability throughout the research lifecycle.
- Ensuring all research team members are trained to use the data capture system appropriately.

8.0 Data Storage

8.1 Research data

The following principles of data storage should be adhered to:

- Use secure storage systems (e.g. encrypted servers, institutional repositories, validated systems, password protected);
- Implement access controls to restrict data to authorised personnel (maintain logs of access, including dates);
- Ensure regular backups and disaster recovery plans;
- Use standardised file naming conventions and folder structures; and
- Local/institutional polices must be adhered to.

While OneDrive can be useful for short term access and collaboration, it is not suitable for long term storage of research data. Files stored on OneDrive are not backed up and data may be lost permanently if the associated user account is deactivated - for example, when a researcher leaves the University.

Research data should be saved in an appropriate area of the UoL Research File Store (R:drive). This area is secure, backed-up, and centrally maintained by the UoL Digital Services.

If you are unsure about where in to store your data, please visit the following webpage:

- https://uniofleicester.sharepoint.com/sites/get-it-help/SitePages/where-store-files.aspx
- https://uniofleicester.sharepoint.com/sites/Research-Governance-Ethics-Integrity/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FResearch%2DGovernance%2DEthics%2DIntegrity%2FShared%20Documents%2FREGI%20Office%2FNon%2DREGI%20documents%2FNHSDataMgmtGuidance%5Fv1%2D1%5F29062022%2Epdf&parent=%2Fsites%2FResearch%2DGovernance%2DEthics%2DIntegrity%2FShared%20Documents%2FREGI%20Office%2FNon%2DREGI%20documents (for research processing data form the NHS specifically).

8.2 Contacts Databases

Where participant contact details are stored for the purpose of contacting individuals regarding their involvement in a trial, these must be stored securely and separately from other research data. Linkage between contact information and research data must be maintained only through a secure code, e.g., participant ID number.

Ideally contacts databases should be stored at the relevant research location. Where contact details will be stored elsewhere, or will be shared, this must be explicitly stated in the Participant Information Sheet (PIS) and Informed Consent Form (ICF).

Access to the contacts database must be strictly limited to research team members who require it for legitimate trial purposes. Access permissions must be role-based, reviewed regularly, and removed when no longer required.

Contact databases must be retained only for the minimum period necessary to complete participant communication and study administration. Once no longer required, contact data must be securely destroyed in accordance with the University's retention schedule and disposal procedures.

9.0 Transfer and Sharing of Data

The UoL's approved system for transferring files to colleagues and external collaborators is Filedrop. This secure platform is designed to support research activities while ensuring compliance with data protection regulations. All document transfers via Filedrop must be encrypted. Before sending, ensure that files are password protected, and always send the password in a separate email.

If you need to transfer large datasets that exceed Filedrop's size limits, please contact Information Assurance Services for further guidance: ias@le.ac.uk

Information about Filedrop can be accessed here: https://filedrop.le.ac.uk/

Please note: services such as Dropbox are not endorsed, as they do not meet the necessary requirements for GDPR compliance, particularly when transferring personal or special category data. In addition, the use of unencrypted portable devices (e.g. external hard drives/Dictaphones) should be avoided, however there may be some instances where this is the most feasible option. In such cases, the information should be transferred to a long-term secure location and purged from the portable device as soon as practically possible.

Where data is transferred into or out of the UoL an appropriate contract must be in place prior to the transfer.

- Data transfer for research location = use the relevant standard HRA template agreement (i.e., OID, mNCA as determined during the Sponsor review process);
- All other transfers (i.e., collaborators, third parties, service providers) = contact the Pre-Award and Contracts team (clspac@le.ac.uk, csepac@le.ac.uk or cssahpac@le.ac.uk) or Procurement Team (procurement@le.ac.uk).

For advice on safe data transfer please contact Information Assurance Services (ias@le.ac.uk) prior to submitting your protocol/DMP for Sponsor review. This will prevent delays during the Sponsor review process.

10.0 Archiving

It is essential that research data is retained in accordance with the legislation and in a way that enables its retrieval during the event of inspection or audit.

SOP S-1032 should be followed.

11.0 Development Record

The table below summarises the revisions introduced in this version. Full historical change records are available within archived SOP versions.

Date	Version number	Description of changes
		• Change of title to 'Data Governance' to more accurately reflect the content of the SOP • Major revisions throughout to clarify data management planning requirements. • Removal of responsibilities table as responsibilities are laid out within the body of the SOP. • Removal of full historical SOP review record; only the latest approved revision is now displayed, with prior versions retained in the document archive.