University of Lancashire

Human Participant Research Data Management Policy Statement

Document type	Research and Knowledge Exchange Service
Document owner	URKEEC
Approved by	14/05/2025
Approval date	Annually
Review date	
Version	1.3
Summary of changes	• Clarified ethical versus UK GDPR consent requirements. • Included EU GDPR guidance for EEA-based research. • Updated secure data storage requirements (approved platforms, LIS backups). • Clarified secure handling of physical documents. • Updated ICO anonymisation guidance references. • Clarified UK GDPR consent withdrawal procedures.

University of Lancashire
Human Participant Research

1. Scope

The purpose of this document is to inform researchers about the process of research data management, before, during and after completion of a research project and sharing research data which concerns human participants. The data generated, which will be of varying levels of sensitivity depending on subject matter, will require a level of protection that adheres to research data management compliance regulations and external funder policies. Guidance[1] has been developed which looks specifically at sharing data from Human Participant Research, in addition to this, the Research Data Management Officer can offer advice on any aspects of this addendum which relates to managing/sharing research data.

This policy applies to staff and postgraduate research students.

2. Statement

The University of Central Lancashire supports the principles of Open Access to publicly funded research outputs and the data underpinning this research. Research data generated at the University is recognised as an institutional asset that when shared openly not only increases the visibility of the University's research but also facilitates public engagement and creates new opportunities for knowledge exchange and collaboration.

3. Responsibilities

All researchers should familiarise themselves with relevant University policies, in particular the Research Data Management Policy, the Open Access Policy, the Policy on Intellectual Property for staff and students, the Data Protection guidance for researchers[2] and Ethical Principles for Teaching, Research, Consultancy, Knowledge Exchange and Related Activities.

Overall responsibility for research data management during any research project lies with the most senior researcher (the PI/data steward for the project). In cases where the project is led by an external partner there is still a requirement for data generated or shared by the University to be managed by a named individual at the University. Researchers should familiarise themselves with the Data Protection guidance for researchers to ensure all personal data, whether stored in electronic or physical form, is kept secure and disposed of appropriately

4. Research Data Management

Staff/researchers are advised to refer to the University's Research Data Management Policy which requires data sharing[3] wherever feasible. When sharing research data, the following principles of good practice are recommended.

[1] This guide will be made available once the policy has been approved, this will include an appendix, which will provide suggestions for wording consent forms in a way which permits data sharing.

[2] See page 14, "Where can my research data be stored?" This guidance clarifies that any paper-based materials (e.g. consent forms) must be kept in a secure location with restricted access, protected from damage (e.g. moisture/heat), and outlines who is responsible for handling or disposing of them if a researcher leaves the University.

[3] Guidance on selecting data for archiving and sharing on Open Access http://clok.uclan.ac.uk/14212/

4.1 Prior to the commencement of a research project

4.1.1 Prior to commencement of a research project or trial, the project team must ensure that data management is fully considered and that good practice guidelines are followed.

4.1.2 Ethics approval should be in place relating to data collection, retention and subsequent sharing.

4.1.3 Before starting a new research project, the PI/data steward and project team must address the following data management requirements:

a) All research projects (including trials) that involve human participants should adhere to the University Open Access Policy, Research Data Management Policy, Ethical Principles, Code of Conduct for Research and Data Protection Policy, and take into account the Data protection guidance for researchers.

b) As stated in The University's Research Data Management Policy, all research projects whether funded or unfunded should have Data Management Plans in place.

4.1.4 Standardisation of data collection and management (including anonymisation protocols) and plans for data sharing should be formulated and documented. Researchers should note that, from a UK GDPR perspective, truly anonymised data are not personal data and therefore do not require consent to share for data protection purposes. Where data are not fully anonymised, researchers must ensure that sharing meets UK GDPR requirements (for example, relying on a lawful basis such as 'public task' for research) and that participants are made aware of how their data will be used. For more information on best practices for anonymisation, please see the ICO's anonymisation guidance.

- Important distinction: Ethical consent to share data is often still required for participant protection and transparency, but this is separate and different to UK GDPR consent to process personal data. When relying on UK GDPR consent as the lawful basis, it must be freely given and capable of being withdrawn; if data cannot be isolated and withdrawn later (e.g., in a public repository), then UK GDPR consent is unlikely to be appropriate. Please see the Data protection guidance for researchers for further information.

4.1.5 Where permissible, costs of data storage and anonymisation (particularly for qualitative data) should be estimated and included in funding bids. Some funders may allow for these additional expenses, and the UK Data Service's anonymisation costing tool can help with planning. Anonymising interview transcripts or similar materials may require extra resources or specialist tools. For support or advice on data storage costs, please contact LIS prior to commencing a research bid.

4.1.6 When planning for the management of data collected from research participants, the PI/data steward and project team have an ethical and legal responsibility to ensure that confidential and personal data are shared and stored securely and that these are not disclosed to unauthorised persons. All personal data from a project/trial must be handled in compliance with Data Protection legislation, and Data Protection principles should be followed.

4.1.7 During a project/trial when sharing personal data, researchers must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Note that when collecting data from participants who are in the European Economic Area, researchers may also need to comply with the EU GDPR, particularly if collaborating with a partner based in the EEA. Researchers must also comply with the Human Tissue Act (HTA)

2004 and the Medicines for Human Use (Clinical Trials) Regulations 2004 where applicable.

4.1.8 All research conducted in the NHS should comply with the UK Policy Framework for Health and Social Care Research.

4.1.9 There is an ethical requirement that consent is obtained when collecting data from human participants. This is distinct from consent used as a lawful basis under the UK GDPR. See the Data Protection guidance for researchers for further information.

4.1.10 Protocols on obtaining informed consent from participants should be followed for data sharing and long-term preservation/curation where possible. Consent forms should include appropriate consent for anonymised data sharing[4]. Informed consent for data sharing and long-term preservation should be made clear in the Data Management Plan[5]. The project funder may also have specific consent requirements which should also be adhered to.

4.1.11 All participant data must be stored in secure locations owned, managed, or approved by the University. This will typically include University shared network drives or Microsoft 365 (MS365) cloud storage, which The University has arranged via approved suppliers.

- Researchers should not store data on external personal/cloud drives that have not been approved by the University.
- In instances where data subjects/data are outside the UK, participants should be informed about where their data will be stored, and researchers must ensure that any international transfers comply with UK GDPR requirements.

[Note: We recommend verifying current backup arrangements for MS365 with LIS. (At the time of writing, MS365 data is backed up by the University.)]

4.1.12 The participant(s) should be informed what the project team will do with the research data collected throughout the project and beyond. Participants should be advised of their rights regarding their research data, including the right to withdraw consent and the time parameters beyond which this consent cannot be withdrawn as the data has been anonymised and anonymisation protocols applied.

4.1.13 Researchers should ensure that accurate information regarding participants is available, including consent forms that include appropriate consent for data sharing.

4.1.14 Retention periods for primary/raw data and related material should be considered at the outset and should reflect institutional, legal and regulatory requirements and, where possible, aim to support new research. Most major research funders have guidelines or requirements regarding data retention periods that you must ensure you follow.

4.1.15 PI's/data stewards and the project team have a duty to the University, and current and future participants of the study, to ensure that the results of the study are adequately managed. Failure to do so may be regarded as a form of research misconduct.

4.1.16 All funded projects should comply with their funder's data management and sharing policies. As per the University's Research Data Management Policy, in cases where researchers may be affected by a number of policies, external funder policy should take precedence; however you must note that funder policies do not override legal requirements

[4] Consent forms must be retained securely for the length of time designated at the onset of the research project/trial and in line with any funding body requirements.
[5] Funder DMP templates are available here: https://dmptool.org/public_templates

so you must ensure you comply with legislation such as the UK GDPR when meeting external policy requirements.

4.2 Data Management during a research project

4.2.1 To ensure the safe storage of data during a project/trial, you must comply with current information governance and LIS guidance, including encryption/restricted access[6]. Both local network storage and MS365 applications such as OneDrive and Teams will ensure research data remains secure, if they are set up correctly. OneDrive for Business is the only University-approved cloud storage and sharing tool. Network storage has automated backup. Both sensitive/confidential data can be stored in these locations.[7] . For more information about how to manage data safely, contact the Legal and Governance team.

4.2.2 Some projects will have designated databases for live data storage[8]. For practical guidance on file naming, version control, and metadata, please consult the Research Data Management SharePoint site.

4.2.3 From an ethical standpoint, participants need to understand the possible future uses of their data. This requirement to be transparent about future uses is separate from any lawful basis under the UK GDPR. Most personal data used for research will be processed in reliance on the lawful basis of 'task in the public interest' rather than 'consent'. For this reason, it is important not to conflate ethical consent with the lawful basis from the UK GDPR on which you rely to process participant personal data.

- The participant information sheet/consent form should include details of any anonymisation, the extent of planned sharing, future data storage and conditions of access.

The table below summarises the key distinctions between ethical consent and UK GDPR consent used as a basis to process participant personal data, helping researchers develop appropriate participant information sheets and consent forms that address both ethical and data protection requirements. Note that consent as a basis on which to process personal data for research purposes is not recommended, in most cases.

Dimension	Ethical Consent	UK GDPR Consent
Regulatory/ Legal Basis	Grounded in research ethics frameworks (for example, the Declaration of Helsinki) and institutional ethics policies. Not mandated by data protection law.	One possible lawful basis under the UK GDPR (Article 6(1)(a) and Article 9(2)(a) for special category data) on which to process personal data.
Purpose	Ensures voluntary, informed participation, respecting the autonomy and well-being of participants.	Permits personal data processing for specified, transparent purposes (if consent is chosen as the lawful basis) Must be freely given, fully informed and capable of being withdrawn at any time.

[6] Research data can be encrypted, and password protected by using the software 7-Zip, which is recommended by LIS.
[7] Under certain circumstances, i.e. for sharing data with external collaborators, contact LIS for further advice.
[8] For example, CTU uses REDCAP

Dimension	Ethical Consent	UK GDPR Consent
Scope	Covers the participant's agreement to take part in the overall research project, including methodology and dissemination. Does not specifically relate to the processing of participant personal data for UK GDPR purposes.	Applies specifically to the processing of personal data (collection, storage, sharing, etc.). Does not cover other aspects of research ethics.
Withdrawal	Participants can withdraw from the study at any point if they do not wish to continue, affecting their ongoing participation. If participant personal data are processed in reliance on a lawful basis other than consent (such as public task) their withdrawal of consent to participate does not affect the use of personal data collected up to the point of withdrawal.	If UK GDPR consent is the chosen lawful basis, participants can withdraw consent to personal data processing at any time, which requires you to stop that processing and delete the personal data (unless it has been fully anonymised). Once consent is withdrawn, you cannot switch to a different lawful basis to continue processing the same personal data; the processing must cease.
Consequences of Refusal	If a participant refuses ethical consent, they simply do not take part in the research.	If participants are asked to consent to the processing of their personal data but do not give UK GDPR consent, you cannot lawfully process their personal data.

4.3 Data management after the completion of a research project

4.3.1 Post-project consent for participants' anonymised data to be made public should be addressed in the original information participants received and documented on consent forms. Participants should be informed and consent at the onset if datasets will be intended to be included in a research depository or to a data archive. Note that truly anonymised data (data which is not capable of being used to identify someone, either on its own or when combined with other information accessible to the viewer) are not personal data under the UK GDPR, however under an ethical perspective you should still gain participants consent for sharing data. If ethical consent is not received for sharing anonymised data, then that data should not be subsequently included in the data to be made Open Access.

4.3.2 If datasets can be anonymised, and approval has been obtained from the appropriate Ethics Committee and/or the Confidentiality Advisory Group (CAG) where applicable, data can be prepared for data-sharing and lodged in an appropriate repository. It is recommended that the designated repository is UCLanData[9] unless a funder or publisher requires an alternative location.

[9] http://uclandata.uclan.ac.uk/ please be aware that a funder may require data to be deposited in specifically named data repository (for example ESRC require deposit of data in the UK data archive).

4.3.3 Once data have been truly anonymised for publication, participant permission is not required for future work on the specific dataset(s). Note that it can be very difficult to anonymise qualitative data relating to human participants.

4.3.4 If data cannot be anonymised, it should be stored securely in a location owned or managed by the University that is backed up[10] and access is restricted to designated project/trial team members[11] . See LIS guidance on where to store files for further information.

4.3.5 Personal data from a project/trial should be securely destroyed when there is no business, regulatory or archival reason for retaining it. Participants should be informed in the participant information sheet and the research privacy notice about how long their personal data will be retained in identifiable form for the purposes of research. Researchers should clearly distinguish between the personal data that will be held securely and ultimately destroyed, and anonymised research data that will be retained indefinitely and made available to others. Consult the Information Governance pages of the University intranet for the current guidance or contact the Information Governance team on DPFOIA@uclan.ac.uk for further advice.

4.3.6 Under Data Protection legislation, personal data from a project/trial should not ordinarily be retained for longer than is necessary for the purposes for which they were originally collected. Personal data held for archiving, scientific or historical research, or statistical purposes may be retained indefinitely if certain conditions set out in the data protection legislation are met. Check external funder retention guidance and the University's retention schedule for guidance on setting appropriate retention periods.

4.3.7 A metadata[12] only record can be created in UCLanData for final project data[13], except in any instance where disclosure of descriptive metadata about the research participants may impact individuals' privacy/identify participant(s); in this case a metadata record should not be created on UCLanData.

4.3.8 If the research funder has an open data policy, the funder should be informed as soon as possible about plans for sharing or safeguarding data.

4.3.9 A designated data steward is required for each project. It is recommended that the PI is automatically assigned as the data steward. Where the student is named as the Chief Investigator in applications requiring approval the Health Research Authority, the data steward named should be the Director of Studies or Academic Supervisor.

5. Sharing Research Data

5.1 Each research project/trial that involves human participants, and where consent for sharing research data is a requirement, should be reviewed on a case by case basis by the Committee for Ethics and Integrity, via the Ethics Review Panels.

[10] Data is backed up daily overnight.
[11] Access to the university shared drive data and hence folders is managed using groups, access is controlled by the owner of the shared area.
[12] Details the characteristics of, for example, a dataset. It is a bibliographic description of the record for resource discovery and preservation.
[13] This is where the details of the project or trial data are recorded in UCLanData. It is a descriptive record of a research data output without any file attached/the file may be restricted.

5.2 Obtaining consent to share research data should be an integral part of the consent process. In cases where data sharing is not possible, researchers should explore alternative options to make subsets of the data available. The PI/data steward should provide a valid reason to opt out of Open Access. In cases where data cover sensitive topics and cannot be shared, it is the responsibility of the PI/data steward to inform the Research Knowledge and Exchange Governance Sub-Committee, via the Ethics Review Panels, before commencement of the project. If all options to make a subset of the data open have been explored, and it is still not possible to share the data, then this data may be exempt from Open Access. However, if there is a funder requirement, the researcher should instead use the statement as an explanation of why the data cannot be made accessible[14].

5.3 In some cases, data may be rendered inaccessible until after a specified period of time[15] has elapsed with a 'request a copy' option - this must be agreed by the Research Knowledge and Exchange Governance Sub Committee via the Ethics Review Panels.

5.4 In some cases, data may require access control[16] and access to specific data may be closed/restricted. Access to this data would be on a case by case basis and should meet funder and University data sharing requirements and criteria[17].

5.5 Data will be maintained in perpetuity within UCLanData (unless the funder or commissioning body dictates a specific period of retention). If the PI/research team are not available because they have left the University, decisions on whether to grant requests for access to restricted access dataset(s) will be taken by the Research Knowledge and Exchange Governance Sub Committee via the Ethics Review Panels.

5.6 A notification on how to request access to a closed/restricted dataset(s) should be clearly visible on the individual UCLanData record so that the user can follow the appropriate access control routes.[18]

6. Research Data Compliance

6.1 All funding bodies (and other stakeholders) should be acknowledged on the UCLanData record. Where sharing is covered by a data sharing agreement, researchers should refer to the agreement for guidance.

6.2 If research publications are produced as a result of the research project/trial then the publisher/journal data sharing policies should be checked to ensure that they are compatible with the University's Open Access Policy, Research Data Management Policy, funding bodies' criteria and Clinical Trials Regulations (if applicable). An alternative publishing outlet should be sought where policy requirements are not met.

6.3 A metadata record of all dataset(s) should be recorded in UCLanData (even if the dataset(s) cannot be made Open Access) unless the project team can provide a valid reason to the

[14] For example: children, vulnerable adults.
[15] An embargo period can be set on UCLanData, and the data will become available on Open Access once the embargo period has lapsed.
[16] There are three tiers of access control i.e. open data, restricted data and controlled access data. These are outlined in the guidance document.
[17] The committee will set the University's criteria, anticipate some of the criteria will only be shared with bona fide researchers, the research project brief meets the criteria for access, PI/data steward agrees with access being granted and must also ensure that funder requirements are met.
[18] Relevant guidance will be made available.

Research and Knowledge Exchange Governance Sub Committee, via the Ethics Review Panels, for not doing so.

6.4 Some funders specify time frame parameters for exposure of data after completion of trials - researchers are expected to comply with these parameters.

6.5 Deposited data should indicate whether the data will be retained in perpetuity or made openly available only for a specified time period as per external funder requirements.

6.6 Data deposited in a data repository should follow standard formats. See UK Data Service guidelines.

6.7 A data access statement is required for each project/trial. If access to the data is restricted this should be justified in the data access statement.

6.8 Supporting documents must be made available in the UCLanData record to facilitate analysis and re-purposing of data such as a readme file/access key and a data dictionary so that the data can be re-usable and understood by a user, see UCLanData guidance for further information.

7. Legal, contracts and agreements

7.1 When working with research data, researchers must be aware of legal issues surrounding research data, particularly sensitive and personal data.

7.2 When receiving, sharing, acquiring, or generating sensitive and personal data, the PI/data steward and project team may need to enter into various contracts with external third parties and partnership institutions.

7.3 The PI/data steward and the project team should be aware of research data terms and conditions contained in documents and consult with the Legal and Governance team for further advice as required.

8. Intellectual property and rights relating to research data

Intellectual Property Rights (IPR) (e.g. copyright, patents) affect the way that the research outputs can be used by the project team and other parties. In general, raw data on their own are considered facts and thus cannot be copyrighted. However, data that are gathered together in a unique and original way, such as databases, can be copyrighted or licensed. It is important to understand data licensing[19] from the perspective of both the data user and data creator when collecting data and sharing data. Ownership of Intellectual Property (IP) created by University staff is outlined in the University Policy on Intellectual Property (Section 3).

9. Data Protection and related policies

The University currently has various documents and policies which refer to different aspects of research data management. If a researcher's data contain personal data (information that relates to a living individual(s) where the individual(s) can be identified from those data or from those data and other information that is reasonably available) then researchers must comply with Data Protection legislation. Data Protection legislation in the UK is the UK GDPR and the Data Protection Act 2018. If a researcher processes personal data about individuals who are physically in the European Economic Area, the researcher may also need to comply with the EU GDPR, particularly if working with a partner

[19] Creative Commons License - https://creativecommons.org/licenses/
Open Data Commons License - http://opendatacommons.org/licenses/

that is based in the EEA. Key University guidance documents and policies can be found here: Data Protection guidance for researchers, Data Protection Policy, Email Use Policy, Information Management Policy, Data Protection Checklist, University code of conduct for research and the IT Security Policy.

9.1 Freedom of Information

Any information held by or on behalf of the University can be requested under the Freedom of Information Act 2000. In some cases, information requested may be exempt from disclosure, particularly if it relates to an ongoing programme of research and its disclosure into the public domain at the time of the request would be prejudicial to the research or to another party. Each request must be considered on its own merits. Any information disclosed in response to a request is disclosed into the public domain. All requests under the FOIA will be handled in line with the University's Freedom of Information Policy and managed by the Information Governance team.

10. Statement Review

The Committee for Ethics & Integrity (CEI) will be responsible for approving this policy statement as recommended by the Open Research Steering Group. The policy statement will be reviewed at least annually by the Open Research Steering Group and updated as deemed necessary.

Next Review date [TBC]