

Research data toolkit

A guide to handling research data safely, effectively and legally



This guide is aimed primarily at Masters of Research and PhD students, however taught course post-graduate students conducting in-depth or complex research may also find this useful. Undergraduate and taught course post-graduates should refer to our [Research Data Management best practice – quick guide](#).

The Basics: Ready, Steady, Go...and Stop

READY Planning your research	• Check whether you need to complete a research ethics review • Think about if you will be using personal data in your research • Begin thinking about whether you want to make requests under Freedom of Information for your research. • Check if you have specific data security requirements and whether LSE needs to sign off any agreements
STEADY Preparing for data collection and use	• Submit your ethics review (if required) and await approval • Write a DMP or review your existing DMP • Send any agreements from data providers to Datalibrary@lse.ac.uk or personal data sharing agreements to lse.info.rights@lse.ac.uk • If necessary, fill out a Data Protection Impact Assessment • Fill in any departmental documentation or registers • If the research entails travel, complete the Notification to Travel form and have a Cyber Security briefing
GO Conducting your research	• Send queries about data management, storage or security to Datalibrary@lse.ac.uk • Update your DMP and Department with any changes to plans
STOP Closing your project	• Archive and publish and/or delete any datasets (including copies) in accordance with your DMP, project-level data security document, contracts and funder requirements • Once data has been anonymized, archived or published, think about the secure destruction of original data

Planning your research project

Know your data

It's crucial to understand the data you will be working with. Data is anything that supports your final results, including any secondary datasets. Think about the methods you'll use, the data types they will produce, the sensitivity of the data, the dataset's format and size and what tools you'll use to create and work with the data.

Personal data definition

Any data that can be used to identify or is about a natural person is personal data. If you are processing names, addresses, opinions, IP addresses, geographical location to the second, etc you will be processing personal data. This means you have to identify a lawful basis for processing which will be task in public interest or legitimate interests, determine what data you need for your project, ensure that the data is accurate, only kept for as long as you need it and kept secure. You can keep data for research for as long as you think you will need it so let research subjects know if you think you will be keeping it longer than the project you collect it for.

Special Categories personal data definition

If you are processing race or ethnicity, health, religious belief, philosophical belief, political opinions, biometric or genetic data, trade union membership, or data about a person's sexual orientation or sex life, this is special categories data. You need to identify a further lawful basis for processing which will be research.

Using Freedom of Information requests for research

Freedom of Information can be used to request data from public authorities. Once you put in a request, you should get a response within 20 working days. However, some public authorities can take longer in practice, so if you want data quickly, it is better to try other sources. Also, there are exemptions to release which may be used on parts or the whole of your request.

Information security

Handling research data securely is a shared responsibility between researchers, departments and the School. Appropriate information security measures help protect research participants, ensure legal and contractual compliance, maintain research integrity, and safeguard LSE's reputation. Security controls should always be proportionate to the sensitivity and risk of the data being used.

Understanding risk and data sensitivity

Before collecting or accessing data, you should consider:

- The sensitivity of the data (e.g. personal data, special category data, commercially sensitive or politically sensitive data).
- The potential impact if the data were lost, accessed without authorisation, altered, or disclosed.
- Any specific security requirements imposed by funders, data providers, collaborators, or contractual agreements.

Higher-risk data requires stronger security controls and may only be handled within approved secure environments.

Cyber security awareness and training

All researchers and students are expected to have a basic understanding of cyber security risks relevant to research data. LSE provides mandatory and recommended cyber security training via [Moodle](#), covering topics such as data protection, phishing, password security, safe use of devices, and handling sensitive information. Please note:

- Researchers working with personal, sensitive, or restricted data are strongly encouraged to complete the relevant cyber security training modules before accessing or using the data.
- Completion of cyber security training may be a pre-requisite for access to certain secure systems or datasets.
- Refresher training should be completed periodically, particularly for long-running projects.

Details of available training and how to access it are available via [Moodle](#).

Cyber Security advice

Information security advice is available throughout the research lifecycle. Early engagement is strongly encouraged, particularly for high-risk or complex projects. For advice on data storage, cyber security, secure data environments, or incident reporting, contact: dts.cyber.security.and.risk@lse.ac.uk.

Research ethics review

An ethics review is required for any study involving:

- Interviews, surveys, focus groups, experiments, observations of people, etc.
- User generated data (e.g. from discussion forums, social media, vlogs, blogs, comments on posts or articles).
- The collection or use of any personal data/identifiable information (e.g. names, email addresses, IP addresses, social media profiles or meta-data, visual material, etc.). Research that will only use data from publicly available archival

records (incl. newspapers) does not require ethics review (unless there are other reasons why it may give rise to ethical issues).

- Any other information that could identify a living individual (or potentially lead to their identification). E.g. as a result of combining datasets, or where an online search for particular wording could lead to the identification of an individual;
- If findings/conclusions/publication could have damaging repercussions for any individuals (reputation, stigma, bullying) or groups with protected characteristics;
- Any other reason why the research might raise ethical issues.

You must obtain ethics review approval before you commence any data collection.

How to complete your ethics review online:

- Read the instructions and follow the link on the [research ethics webpages](#)
- Remember to reflect on the questions and answer honestly; discuss any questions or concerns with your supervisor, or email research.ethics@lse.ac.uk

Research that may undergo ethics review elsewhere

If your research will undergo ethics review elsewhere (e.g. at another university, or if the research requires HRA/NHS approval), complete the online ethics review form as far as screen E. The Research Ethics Managers will confirm whether or not LSE review/approval is also required.

Preparing for data collection and use

Data collection and use

Ahead of data collection, consider any dataset terms and conditions, participant consent, software/hardware, and services involved in data collection.

You may also be working with data with additional considerations:

- **Secondary data:** Plan for any costs and follow any terms and conditions, whether that is [data via LSE Library](#) or other accessible data. Consider copyright or any other usage restrictions.
- **Personal data:** This will include direct identifiers (e.g. names, addresses) and indirect identifiers (Combinations of data that disclose someone's identity). Don't collect more than necessary and store consent, personal data and anonymised data separately in password protected folders in LSE OneDrive.
- **Social media data:** This is personal data, so we recommend reviewing these two guides: [LSE Social Media, Personal Data and Research Guidance](#), and [Using data from the internet and social media: ethics and consent](#).
- **Secure data:** Check our [secure data access](#) webpage for full guidance.

Data Sharing Agreements

You may be required by data providers to enter into a data sharing agreement which sets out your responsibilities for sharing the data. The agreement should cover who will be doing what with the data, what the data is, transfer mechanisms and how long the data can be kept.

- For **personal data sharing** only you may be provided with a template by the data provider or you can contact the Data Protection Officer for the School's template. The DPO can advise on any amendments to the DSA proposed and the School Secretary will sign.
- For **controlled or confidential data agreements** you may be provided with a template by the data provider and contact the [datalibrary](#). Agreements that require institutional signature will require review by Legal Services and Cyber Security.

Informed consent

Informed consent is widely accepted as the cornerstone of ethical practice in research that involves human participants or personal data. The informed consent process should stress that participation is voluntary and can be ended at any point during the research (although you may need to qualify that data can only be withdrawn up until a certain date when analysis will begin and/or publication).

Your information sheet and consent forms (whether provided in written or verbal format) should include clear information about data management, use and sharing.

Please refer to the [LSE guidance on Informed Consent](#) (includes sample templates).

There may be some circumstances where gaining informed consent is not possible – for instance, in the case of fieldwork or ethnography in some public or online spaces - but in these cases, justification will need to be provided to the Research Ethics Committee.

If your research will involve children or vulnerable groups, please also refer to the LSE guidance on '[Research with children and other vulnerable groups](#)' as well as the LSE [Safeguarding in Research and International Activities Policy](#).

Approval of your ethics review

Applications are automatically categorised as requiring either Departmental (incl. Research Centres and Institutes) or Research Ethics Committee review/approval:

1. Departmental review

Applications that raise few ethical issues will be automatically routed to Departmental review/approval. For students, such applications will be reviewed by the project/ dissertation/thesis supervisor (or academic mentor/advisor) as appropriate.

2. Research Ethics Committee (REC) review

Applications for projects that include any of the following elements will be categorised as requiring review/approval by the Research Ethics Committee:

- sensitive topics that participants may find emotional or distressing.
- the involvement of children or other vulnerable groups;
- research that poses a risk (whether physical or emotional/psychological) to either the participant or the researcher beyond that normally encountered;
- deception or the withholding of information as to the true purpose of the study;
- where consent will not be obtained in writing (this does not apply to researchers in Anthropology).

MSc student projects which are not for dissertations, and all UG projects, are exempt from REC review, unless the supervisor has concerns and refers the application to the REC.

Data management planning: A Data Management Plan (DMP) is a document outlining how data will be collected, used, stored and shared during and after research projects.

A DMP must be completed if:

- An external funder requires it at application or award stage.
- You are accessing secure data that requires a data sharing agreement.

- You are accessing internal LSE data.
- The Research Ethics Board requests you complete a DMP

Please see [DMPOnline](#) for templates. If you are planning a funding application, [check what your funder requires](#) as they often have very specific templates.

To receive advice tailored to your project submit your data management plan to us for review via the share tab in DMPOnline. The review service is primarily for PhD Students and research staff, however some Undergraduate or Postgraduate Taught course student projects may require review. For more information see the [Quick Guide to DMPs for UG/ PGT students](#).

Data Protection Impact Assessments: You may be required to conduct a [Data Protection Impact Assessment](#) (DPIA) by a funder, data provider or because your research could have significant effects on a person. The DPIA goes through what you propose to do, what the risks are and how you will mitigate them. The first part consists of screening questions as to whether a DPIA is needed. The second part goes into detail about the risks and mitigations and how you will incorporate the mitigations into your research. The Data Protection Officer can help you through this process.

Conducting your research

Research tools

Carefully consider your research tools to ensure they are compliant with LSE's requirements. Researchers must ensure that tools used to collect, analyse or process data meet LSE security requirements:

- Only use tools that are approved or recommended by LSE, particularly for sensitive or personal data.
- Take particular care with tools powered by Artificial Intelligence (AI) - see below, transcription services, or external Software-as-a-Service (SaaS) platforms, as these may involve data being processed or stored outside LSE's control.
- If unsure, seek advice before using a tool with research data.

For details of LSE-recommended research tools please see the [Specialist Research Tools](#) webpage. webpage.

Usage of AI research tools

First consult your academic department to confirm whether AI tools are permitted in your research and use any approved tools in line with the [School's AI Legal and Regulatory Guidance](#).

You must use LSE-supported tools wherever possible, Microsoft Copilot for staff and Claude for students and teaching staff.

If you do choose to use external LSE unsupported AI tools, you must never upload any commercially sensitive, personal or copyrighted data to them. If the tool is used in a manner that breaches GDPR or any other data protection laws, or School policies, you may be personally accountable for any resulting issues, including data breaches, unauthorised processing, or noncompliant handling of personal information. You must review vendor's privacy, security and contractual documentation at least twice a year to ensure they are still compliant.

Wider use within a team, department or teaching context requires approval from DTS, an A.I Assessment and completion of Cloud Assurance Questionnaires, which can be found on the [IT Policies webpage](#).

Secure access and storage

Researchers must use LSE-approved systems and services to store and process research data:

- Use LSE OneDrive, SharePoint, approved cloud platforms or secure research environments as appropriate to the data classification.

- Do not store sensitive research data on personal devices, unmanaged cloud services, USB sticks, or personal email accounts.
- Ensure that encryption is enabled where required and that access is restricted to authorised project members only.
- Apply the principle of least privilege: only give access to those who genuinely need it, and remove access when it is no longer required.

For datasets subject to additional controls (e.g. secure or restricted data), follow the guidance on the [Secure Data Access](#) webpages.

Accounts, access and authentication

- Do not share user accounts, passwords, or access credentials.
- Use strong passwords and multi-factor authentication (MFA) where available and required.
- Review access regularly, particularly for long-running projects or where staff or students leave the project.

Data transfer and sharing

When transferring or sharing research data between collaborators:

- Use secure transfer methods approved by LSE (e.g. encrypted file transfer services or secure portals).
- Avoid high-risk methods such as standard email attachments or consumer file-sharing services for sensitive data.
- Ensure that any data sharing is covered by an approved data sharing agreement and ethics approval where applicable.
- Do not onward-share data beyond the approved recipients.

Security Incident reporting and support

A security incident includes loss of data, unauthorised access, accidental disclosure, phishing attacks, or suspected compromise of accounts or devices.

If you believe a security incident has occurred:

- Report it immediately via LSE's established incident reporting channels.
- Do not attempt to resolve the incident alone.
- Prompt reporting helps minimise harm and ensures legal and regulatory obligations can be met.

Research Ethics Amendments

If you need to make amendments to a study that has already received approval, you should complete an Amendments form following the instructions available on the

[Research Ethics webpages](#). (If the amendment is very minor or may not have any ethics implications, please email research.ethics@lse.ac.uk in the first instance.)

Organising your data

It is important to organise your data well to ensure managing it during the project's lifecycle is easy, quick and secure. Sensible file names and well-organised folders will make it easy to find and track your files. Define clear and consistent variable names carefully so they can be identified, understood and have meaning. Having accompanying documentation to your data can also provide contextual, methodological and technical information to help understand your data and how it's been created. The UK Data Service have great advice on how to [organise your data](#) and to [document your data](#).

Closing your project

Data sharing [PhD students and academic staff only]

Once the active phase of your project is completed it's important to consider how you can preserve your data and, if possible, share it with others. Where possible, you should deposit any data that underpins research outputs or has long-term value into a data repository. LSE has its own [data repository](#), and the library team provide a tailored and hands-on support service for those new to depositing their data. For further information on this please see our [archiving and sharing](#) webpage.

Data retention and destruction

Your responsibilities for your data don't end when your project finishes. Whether or not you have published or archived your data, you will need to consider data retention and destruction. Generally, researchers are advised to keep research data for 10 years from the end of a research project or the point of publication of your findings for potential peer review purposes. Personal data can be kept after a research project finishes if it might be used in future research. However, sensitive data should never be informally retained "just in case". Please see the LSE [retention schedule](#) for further guidance. When you do destroy data, make sure you permanently delete the data – delete all copies, including those in deleted folders or recycle bins and delete all back-up copies of additional hardware.

Get in touch with your key contacts

Expertise	Name	Title	Contact
Data management plans, secure data access, data access statements, data archiving	Hannah Boroudjou and Julie Baldwin	Research data Librarians	Datalibrary@lse.ac.uk
Research ethics, research conduct	Lyn Grove	Senior Research Ethics Manager	Research.ethics@lse.ac.uk
Data protection, freedom of information, information and records management	Rachael Maguire	Records Manager	lse.info.rights@lse.ac.uk
Data storage and security, cyber security, secure data	Muslim Saadat	Head of Information Security	dts.cyber.security.and.risk@lse.ac.uk

Come and meet us at our weekly drop ins!

If you have any questions at all about data management that have not been answered by the Toolkit then feel free to join one of our weekly data drop-in sessions. These are online sessions which run throughout the term and give you a chance for a 1-2-1 with the Research Ethics managers, the Data Protection Officer, the Law & Copyright Librarian and a Research Data Librarian. Sessions are bookable through the [LSE Life booking system](#) please contact datalibrary@lse.ac.uk for more information.

Review Schedule

Review Interval	Next review due by	Next Review Start
Every 3 years	September 2029	July 2029

Version history

Version	Date	Approved by	Notes
1	04/02/2022	HB	
2	04/02/2022	HB	
3	01/02/2023	HB	
4	02/02/2024	HB	
5	07/01/25	JB	
6	25/09/26	All involved	

Contacts

Position	Name	Email	Notes
Research Data Librarian	Hannah Boroudjou and Julie Baldwin	datalibrary@lse.ac.uk	

Communications and training

Will this document be publicised through Internal Communications?	Yes
Will training needs arise from this policy?	No

