THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Technical

Research Tools Minimum Standards

Introduction

This document outlines the minimums information security standards required when using tools to collect and analyse the research data. Automated data collection and analysis via software and applications is often an inseparable part of research activities, which can have implications for the confidentiality, integrity, and availability of LSE-owned research data, or data provided by third party data providers via a data sharing agreement. LSE-owned data includes datasets provided by the LSE, or primary data collected by/from end users, as part of research and course study.

Purpose

The primary purposes of this Minimum Standard are to:

1. Provide safeguards for using tools to facilitate research data collection and analysis.
2. Provide a basic understanding of the implication for data confidentiality, integrity, and availability when using these tools.
3. Protect the confidentiality, integrity, and availability of LSE-owned research data.
4. Protect the confidentiality, integrity, and availability of data provided by third party research data providers and assist the fulfilment of data security requirements imposed by research funders and data providers.

NOTE: where data provider and/or research funder requirements exceed or conflict with the minimum standards outlined below, the data provider requirements take precedence.

Scope

This Minimum Standard is intended for:

1. All LSE members
2. Software and applications that are not centrally provided by the LSE but commissioned by research staff for specific purposes when collecting and analysing the research data.

Minimum Standards

Cloud Storage

Any LSE data should be stored in LSE-provided storage, including:

- Microsoft SharePoint
- Microsoft One Drive for Business
- Microsoft Team
- H: space
- Departmental shared folder (for staff only)

Any data sharing with external collaborators should be via one of the following means, which allow the LSE user to add a guest account to the data that are shared:

- Microsoft SharePoint; or
- Microsoft One Drive for Business; or
- Microsoft Team

Note that the LSE provides a secure file sharing service via filedrop.lse.ac.uk which is suitable for one-off data transfer.

Where data are internally or externally shared, access to the data must observe the following principles:

- 'need to know' - access is only given to these who have the legitimate business need for such access
- 'least privilege' - access permission level should be restricted to what are absolutely necessary (e.g. Read only vs. Edit)
- The access is 'role based' - access is assigned via user groups instead of being assigned to individuals
- Access permission should be regularly reviewed, to ensure only the right people have access to the right resources for right amount of time

Audio and video recording

This section should be read in combination with the School's Audio and Video Recording Guideline

The following should be followed as a minimum:

Recording device – dictation device

1. If dictation device is used, the recording device is kept in a safe place when unattended.
2. Models with real-time encryption capabilities include:
    - Olympus DS -7000
    - Olympus DS -3500
    - Phillips DPM 8000/00
3. For video recording, there is no proven devices that support real-time video encryption capabilities. Video recording represents a higher risk around personally identifiable data; any video recording files should be imported to a computer with adequate protection as soon as possible

Third party recording apps

1. If recording apps are used, ensure the recording files are NOT automatically synchronised into a third-party cloud service, apart from the cloud service that the School centrally subscribes to (e.g. Microsoft Team, SharePoint, One Drive for Business).
2. Any locally stored recording files are in an encrypted folder or reside on an encrypted drive.

[Note] Files are not required to be encrypted if being stored in LSE-provided storage location such as H: space, departmental shared folder, Microsoft Team, SharePoint, One Drive for Business, unless it is explicitly required so by the research data providers or funders, or is deemed as required out of a risk

assessment around the impacts of exposure/breach of such files.

Third party transcription apps

1. Usage of cloud-based automatic transcription software should be avoided if the recorded contents are sensitive, or if the interviewee's identity is sensitive.
2. If, following a risk assessment by the researcher, a cloud-based transcription software is deemed as acceptable to use as part of the research, the following must be observed:
    - Terms of service and privacy policy of the service provider are checked to ensure a reasonable level of assurance exists around the safeguards towards data confidentiality, integrity, and availability.
    - Be aware of what the service provider does with any voice data, understand what data they store, where the data are physically stored, how long the data are stored for, and what the data are used for by the provider. Any use of the personal data beyond the purpose of transcription, for example using the data for improving their voice recognition accuracy, must be informed to the research participant. The transcription of voice data has to be within the UK or the EEA or countries with equivalent level of protections (for an official list of such countries please refer to https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)
3. LSE recommended transcription tools include:
    - McGowans Transcriptions (https://www.mcgowantranscriptions.co.uk/)
    - Konch (https://www.konch.ai/gdpr/)

    If researchers have any potential services they would like to use, please contact dts.cyber.security.and.risk@lse.ac.uk or glpd.info.rights@lse.ac.uk and they will be checked for security and GDPR compliance.

Third party survey solutions

As mandated Mass Research Survey Policy the following must be met:

1. Third party survey tools should be used in precedence over the emailing system while conducting mass research surveys.
2. While choose a survey tool, the service provider's terms and usage policies must be checked to ensure that their processing of data meets Data Protection legislation (refers to General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA 2018)
3. LSE recommended survey tools include:
    - Mailchimp
    - Qualtrics
    - Survey monkey
    - Microsoft Forms (available as part of Office 365)

Content scrapers

If a content scraper is used, the following must be met:

1. Terms of use of the content provider are checked, to ensure the usage of content scraper is permitted by the content provider, or the conditions for using a content scraper are met.

2. Be aware that the content provider might require the explicit consent of their users in order for the content scraper to be used.
3. If it is unclear from the terms of service whether the content scraper is permitted, or under which conditions the usage is permitted, communication with the content provider should be initiated with an explanation of the purpose of the usage of the content provider and obtain their permission as necessary.

Web applications and mobile apps

1. Any web applications and/or mobile apps to be developed for research purpose as a collaboration between the LSE and third parties must be properly assessed against the safeguards towards the data confidentiality, integrity, and availability.
2. The assessment should at a minimum cover the completion of the School's standard Cloud Assurance Questionnaire.
3. The Questionnaire should be checked and assessed by the Cyber Security and Risk team upon its completion. If, following the assessment, the risks are not within the Cyber Security and Risk team's acceptance level, and the Principal Investigator still wishes to use the application, it will be escalated to either the School's Data Protection Officer or the Chief Operating Officer, depending on the type of risk involved.
4. A Data Protection Impact Assessment should be complete if deemed necessary, particularly if:
    - Special categories personal data as defined by the GDPR
    - A new method of processing personal data. New can mean new to the School
    - Large aggregates of personal data from separate sources
    - Or any other of the triggers listed on the form mentioned below

Messenger and social media apps

1. Usage of messenger and social media should be considered in context of the sensitivity of the research topic and identity of the research participant
2. A Data Privacy Impact Assessment should be complete if deemed necessary.
3. Please refer to the Social Media Guidance for the terms and use of a list of social media sites.

New service

If researchers have any services they would like to check out or recommend others use, please contact glpd.info.rights@lse.ac.uk or dts.cyber.security.and.risk@lse.ac.uk and they will be checked and added to the list if considered secure and GDPR compliant.

Accompanying documents

This Minimum Standard is supported by the following documents:

The Information Security Policy and Information Classification Standard, which outlines how to classify data and how data of different categories must be secured.

Data Protection Policy, which provides an overview of data protection requirements under the Data Protection legislation.

The Audio and Video Recording Guideline which outlines the guidelines around audio and video recording while collection research data.

Mass Research Survey Policy, which sets out the minimum requirements that mass research surveys shall adhere to.

Policy on Online Survey Retention which outlines the requirements around retention of the survey data

Doing Primary Research Online which provides overall advices and document references throughout the data lifecycle

Responsibilities

All LSE members
All LSE members are responsible for meeting this Policy over the course of their studying, research, and employment.

Cyber Security and Risk
The Cyber Security and Risk team is responsible to update this Minimum Standard and advising on any data protection and information security queries or requirements.

The team shall be consulted when there are doubts on this Minimum Standard.

Data Protection Officer
The Data Protection Officer advises on any data protection queries or requirements from a legal point of view.

Library
Library ensures above standards, if applicable, were incorporated into the Data Management Plans.

Information Governance Management Board
Responsible for approving information security minimum standards.

Review schedule

Review interval	Next review due by	Next review start
3 years	June 2023	May 2023

External document references

Title	Version	Date	Author
Information Security Policy	3.20	05/07/19	Jethro Perkins

Data Classification Standard	4.3	03/12/18	Jethro Perkins
Data Protection Policy	2.0	26/03/18	Rachael Maguire
Audio and Video Recording Guideline	1.0	27/01/17	Jia Fu
Mass Research Survey Policy	1.2	03/06/20	Jia Fu
Policy on Online Survey Retention	1.0	19/03/19	Rachael Maguire
Social Media Guidance			Rachael Maguire
Data Protection Impact Assessment	4.1		Rachael Maguire
Doing Primary Research Online			Helen Porter

Version History

Date	Version	Comments
07/19	1.0	Initial version. Approved by Information Governance Committee 15/04/19.
03/06/20	1.1	Added in advised transcription tools. Added in section of 'New service'. Added in Version History. Minor wordings. Updated hyper-links

Contacts

Position	Name	Email	Notes
Information Security Manager	Jia Fu	j.fu8@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	**Yes**
Will training needs arise from this policy	**No**
If Yes, please give details	