

LSE Research Laboratory Data Security Agreement

- 1 The LSE has three levels of data classification, 1 Confidential, 2 Restricted, 3 Public. This form must be signed by any member of the RLAB wishing to use data classified as 1 and 2.
- 2 If there is a need for me to hold or process confidential or restricted data, I will inform my Centre manager.
- 3 I will not store, process or analyse any confidential or restricted data in relation to my RLAB work except via one of the Centre's secure servers following authorisation by the Centre Manager. I will never hold confidential or restricted data on a standalone pc, local hard drive or portable storage device/media.
- 4 I will ensure that I have appropriate licences or contract for all data resources I am accessing, that I understand, and I am abiding by any conditions of the licence or contract, and that these are up to date.
- 5 I understand that data contracts are legal documents and that any breach of conditions may lead to legal, professional or financial penalties (including in some cases losing access to funding or resources).
- 6 I will safeguard any password provided to me, whether for accessing the LSE network and services, an external resource or other data source. I will never divulge a password to any other individual, and I will never respond to a request for my password or attempt to influence any individual to divulge their password.
- 7 I will take all necessary precautions to preserve the security of any data and associated materials.
- 8 I will handle all data and other resources in such a way as to protect myself, my department, and the London School of Economics from any legal challenge or loss of reputation.
- 9 I will at no time attempt to identify, or claim to have identified, any individual, household or organisation that may be recorded in the data.
- 10 I will ensure that if I require institutional support for my data license that only a member of staff with the legal status to represent the LSE guarantees the contract.
- 11 I will abide by data suppliers' regulations regarding the destruction of data, in hard copy and electronic format, on completion of a project for which the data access has been granted. The RLAB IT Manager can provide support in this area.
- 12 I will never enable any other person to access confidential or restricted data. I understand that any sharing of sensitive data among licensed users, including subcontracted partners, must be via the IT Manager following confirmation by a centre manager.
- 13 When handling confidential or restricted data I will abide by the Data Protection Act.

- 14 I will cease using any data licensed at a departmental (economics department, RLAB etc), or institutional level (LSE) on leaving the department/institution (or on gaining a new affiliation) until I have renewed my contract in relation to my new role.
- 15 If I have any suspicion that data confidentiality has been breached whether deliberately or by accident, I will report immediately to the Centre or IT managers.
- 16 When accessing remote data repositories, for example the SRS system at the ONS or the Secure Lab at The Data Archive, you will only use the dedicated desktop based at the LSE in 32 Lincoln's Inn Fields that has been formally agreed with the providers. Alternatively, during the Coronavirus pandemic, data providers have agreed that an Institution bought and set-up device may be used to remotely access a dedicated server based at 32 Lincoln's Inn Fields that contains the remote software required to access these systems. Please note this second option is only available during the Coronavirus pandemic and will be removed once physical access to the desktops based at the LSE is organised.
- 17 All ONS accredited researchers MUST take the following precautions during any remote access from home to ONS data held on the SRS or SDS system during the Corona Pandemic lockdown
- They must only work from their agreed nominated UK address,
 - They MUST inform the SRS Research Support team if they access the SRS from a place that is not their home address i.e., an agreed secure room or Government site such as the Bank of England.
 - They MUST NOT leave the laptop unattended or on show, i.e., in a conservatory.
 - ARs MUST Sign off or disconnect from the SRS environment and Remote Access Sessions as soon as they have completed their remote access requirements (this includes taking short breaks etc), laptops must be shut down completely once work has been concluded.
 - Access is only through a machine and connection provided by the researcher's organisation. No use of personal computers is allowed.
 - Access is only allowed where a researcher already has remote access from their organisation approved by ONS under the Assured Organisational Connectivity scheme.
 - No remote access will be allowed outside normal working hours, without prior written agreement with ONS.
 - Approval will be on a project by project basis for individual researchers.
 - Approval to access data to work on a specific research project will not mean that access for any other research project has been approved.
 - Take reasonable precautions to ensure that other household members do not see the laptop screen.
- 18 By accessing and/or using any LSE IT facilities including those of the LSE Research Lab, I agree to be bound by the framework set out in the 'LSE Information Security Policy'
<https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf>
- I certify that I have read and understood all of the above clauses, and acknowledge that my failure to comply with these may lead to sanctions being taken by the LSE in accordance with all relevant School policies, including the Conditions of Use of IT Facilities at the LSE and the appropriate disciplinary policies, in addition to any legal or professional penalties imposed by the data providers. (please tick)
-

Signature:

Print name:

Date:

Email address: