Smart Energy Research Lab (SERL) data

Application guide for SERL data

Table of contents

Introduction to SERL

Smart Energy Research Lab (SERL) Observatory data is accessed through the UKDS SecureLab platform.

Data accessed in this way cannot be downloaded. Once researchers and their projects are approved, they can analyse the data remotely within the SecureLab. We provide access to statistical and office software to make remote analysis and collaboration secure and convenient.

This guide provides details on the application process to access SERL Data only. Guides to access Non ONS and ONS Data are also available on our website.

Introduction to UKDS SecureLab

SecureLab is the UK Data Service's flagship secure environment providing researcher's access to the most sensitive and confidential data in the collection since 2011.

Data accessed in this way cannot be downloaded. Once researchers and their projects are approved, they can analyse the data remotely from their organisational desktop, or by using our Safe Room. We provide access to statistical and office software to make remote analysis and collaboration secure and convenient. We invite data owners and researchers to join the UK Data Service community to enable responsible use of detailed data for high-quality research.

Requirements for access

Researcher requirements

SERL data can be only be accessed by researchers who are able to fulfil the following requirements:

- You must complete Safe Researcher training and have Digital Economy Act Accredited Researcher Status before the project can be approved and access granted (it is recommended you apply for this as soon as possible to speed up the application).
- Postgraduate students can apply however their supervisor(s) must also apply for AR Status.

System requirements

Connection to SecureLab can only be made from a device located at and owned by your institution. The device must have a dedicated static IP address and a wired internet connection (see Technical Checks).

You could also access SecureLab via a Safepod in the Safepod Network (see https://safepodnetwork.ac.uk/ for more information).

About the application process

The application process has a number of components and can seem complicated but is essentially made up of the following four areas that must be completed before access can be granted. These may be completed concurrently as the process can take some time and we will advise you of any outstanding actions and be on hand to answer any queries you may have. Please read the guidance and complete all forms precisely as this will prevent delays to the application.

> **Project application and ethics approval**
> To be completed by the Project Lead

> **User agreement**
> To be completed by each researcher on a project

> **AR status and SRT training**
> Each researcher must complete Safe Researcher Training and apply to ONS for AR status

> **Accessing SERL workspace**
> You will be guided through the set up process

Project application

Submitting an application

- Login/Register with the UK Data Service.
- Add the required Secure Access dataset(s) to your account, then follow the prompts to add the dataset(s) to a registered project, or create a new project. The SERL Observatory data is registered under Study Number 8666.
- Within the project, click Request Access to display the steps to be completed
- Click Complete actions, instructions and links to any forms that must be submitted will be displayed under each step.
- The Project Lead must download and complete the SERL Research Project Application form.
- The Project Lead must complete the ethics self-assessment form (download link can be found in the project application form) and evidence internal ethics approval from their institution.
- Each team member (including the project lead) must download and complete the Secure Access user agreement. If we already have a completed User Agreement on record for you, this step will already be marked as complete.
- Each team member must complete the online SecureLab Account Setup form under the SecureLab Access step.
- Please email your completed documents with your project ID in the subject line to: secure.applications@ukdataservice.ac.uk.

Adding team members to projects

Each team member must be registered with the UK Data Service. The Project Lead can then add each team member to the project. To do this the Project Lead should:

- Log into their UK Data Service account.
- Expand the Data section and then click on Projects.
- Click the relevant project title, where a number of tabs will be visible, e.g. Projects, Datasets, Members.
- Click Members, then New member.
- Enter the UK Data Service registered email address for the team member you want to add.
- Click Add member and their details will be shown in the Project team invitations section of the screen. An invitation will automatically be sent.
- Each team member will receive an invitation email to ask whether they wish to be added to the project.

- Once a team member accepts the invitation to join the project, the Project Lead should check their details are correctly displayed in Project team members.

Each project member will be able to see the project and associated datasets within their own account and should complete any actions required. The Project Lead should collect the Secure Access User Agreements and Ethics self-assessment forms from all team members and email them with the project application form to: secure.applications@ukdataservice.ac.uk. Additional researchers can be added to teams at a later stage with data owner approval.

User Agreement

Completing the Secure Access User Agreement

Before access is given, each team member and a suitable delegated authority in their institution must sign our Secure Access User Agreement. The form can be downloaded under the step Complete Secure Access User Agreement.

What is the Secure Access User Agreement?

The User Agreement is a legally binding contract between you, your organisation and the University of Essex, which is the legal entity for the UK Data Service. The User Agreement was written by the University of Essex's legal team, so we are not a signatory party to the Agreement and we are unable to accept edited versions of the Agreement. The Agreement outlines the terms and conditions of use and includes:

- Agreement that you will complete our training
- Information about your security responsibilities, e.g. not sharing your password, nor disclosing or compromising any Personal Information
- Information about penalties and breaches, set out in our Licence Compliance Policy
- Our outputs release policy
- Our citation and copyright requirements

The Agreement is a 'per person, per organisation' agreement. You therefore only need to complete it once whilst you are at your current institution – if you were to move organisation and still require access to SERL data, then you would need to complete and submit a new Agreement.

Countersigning the Agreement

Your Agreement must be countersigned by someone who can accept legal responsibility for your data access on behalf of the entire organisation. You should therefore approach your organisation's Research and Contracts Office or equivalent, to arrange for an appropriate person to countersign your Agreement. Line managers, PhD supervisors, Heads of Department/School are not acceptable signatories. The exception to this is researchers from the University of Essex, who should ask their Head of Department to countersign their Agreement, as the University's legal team cannot countersign their own Agreement.

AR Status and Safe Researcher Training
Applying for AR status

To access SERL data each team member must have Accredited Researcher Status. Completion of a Safe Researcher Training course is a required to gain AR Status. Applications for AR Status must be made through the ONS Research Accreditation Service (RAS). To make an application please register for an account through the RAS registration system or if you already have one, login to your RAS account. Before we can submit your project application to the SERL Data Governance Board for approval the AR numbers for each team member must be provided.

Completing Safe Researcher Training

The Safe Researcher Training (SRT) course covers.

- Data security and personal responsibility, including legal background, security model, breaches and penalties
- Statistical Disclosure Control - how to make statistical outputs safe and what principles are used
- Using the UKDS SecureLab* - how to use the interface and how to prepare and request data imports and suitable statistical outputs

If you have not attended SRT you will be invited to book on one of our courses. We run these online approximately every three weeks.

If you have trained with another SRT provider within the past 3 years, then we will verify your attendance and you will be asked to complete a short Moodle course that covers the use of our SecureLab.

The SRT course we deliver is valid for Accredited Researcher (AR) applications made via ONS, if you're applying for AR status and are attending training with us, then you can confirm your training date to ONS and they will verify your attendance and successful pass with us before issuing you with AR status. AR status is valid for a period of five years.

If you completed SURE researcher training with the UK Data Service before 1st January 2019 you will need to complete the SRT course as this is the most up-to-date and relevant SRT course to protect data privacy and required to access SecureLab.

If you have not logged into UKDS SecureLab for more than 2 and a half years, you must complete a short online MoodleX refresher course before accessing SecureLab.

Technical Set Up
Completing the SecureLab Account Set Up form

In order to access SecureLab, you must connect from a device located at your organisation/institution.

Each team member must complete the SecureLab Account Set Up form under the SecureLab Access step. When completing the form, you will be asked to submit the following evidence from the office device:

- Screenshot of accessing the web page https://www.whatismyip.com/my-ip-information/
- Screenshot of output of running the command **ipconfig /all** in Command Prompt (Windows) or **ifconfig -a** in Terminal (Mac)

Please speak to your IT department if you are unsure if your device will meet our requirements. Current SecureLab users must complete the form and confirm if the office device has changed when applying for access to a new project.

Technical requirements for SecureLab access

The office device from which you will access SecureLab must:

- Be owned and managed by the institution from which the SecureLab will be accessed.
- Have a direct connection to the internet via a wired Ethernet connection.
- Have a dedicated public IP address that is unique to your endpoint device.
- Have no other network interfaces connected except for the one being used to access the SecureLab, this includes using VPNs.
- Is not running any services which allow third parties to connect to the workstation e.g. a web server or email server.

Researchers must ensure that the following security measures can be observed:

- When SecureLab is accessed, only the wired Ethernet is used, and that the wireless is not connected simultaneously.
- You must only access SecureLab from your designated office, not from any other location on or off campus (see here for information on home working: https://ukdataservice.ac.uk/help/covid-19/covid-19-accessing-securelab-faqs/).
- You must observe good security measures e.g. locking your screens when leaving unattended, not allowing your screens to be visible to people other than SecureLab users working on the same SecureLab project.
- Your SecureLab credentials must not be saved in the web browser.

Processing your application

What happens once you've applied?

Following receipt of your application and evidence, our Data Access team will process your application as soon as possible. Our team screen your application for completeness, including what you intend to do with the data; your proposed use of the data is justified and that your project will deliver clear public benefit.

Once it passes the initial screening, then it progresses to further checks, including feasibility assessment, ethics and methodology checks, if needed.

You might be asked to make amendments to your application if we identify areas which we think need more information or clarification.

When we are satisfied with the quality of the application it will be sent to the SERL Data Governance Board who will review your project.

If the SERL Data Governance Board approve your project, you will be given access to your requested data only for the purposes specified for your project.

We will confirm the decision to you by email. If you have completed all the elements of the application, including attending Safe Researcher training, before we confirm the decision, then you are likely to get access immediately.

Turnaround times

We will start screening your application as soon as possible and keep you informed of the progress of your application throughout the process. The application process starts from when you submit all your application documents to us, rather than when you add the dataset(s) to your project.

If the application is well prepared and approval is granted with no changes required, you can expect to gain access to the data in approximately 3-4 months.

If you require an update on a current application, please email our Helpdesk team, please include your name, institution and the Project ID.

UK Data Service

www.ukdataservice.ac.uk

help@ukdataservice.ac.uk

+44 (0) 1206 872143