UKDS SecureLab: access to ONS data

UKDS SecureLab application guide for ONS Data

12/10/22

Table of contents

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.

This guide provides details on the application process to access ONS data. Guides to access non-ONS and SERL data are also available on our website. If you are applying for Non ONS and ONS data, you must apply for the non-ONS Data first as ONS require evidence that the non-ONS data owners have already approved access.

Requirements for access

Researcher requirements

Controlled data are only available in the SecureLab to researchers who are able to fulfil the following requirements:

- The purpose of the use of the data for your project must provide a public benefit/serve the public good.
- You must check any specific access restrictions for each study in our data catalogue that you wish to use, found in the Access tab.
- Postgraduate students must apply jointly with their supervisor(s).
- You must complete Safe Researcher training and have AR status before the project can be approved and access can be granted (it is recommended you apply for this as soon as possible to speed up the application).

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).

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
The application must be approved by Data Owners

User agreement and ethics checks
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

Technical checks
Carried out on each researcher's office device

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.
- 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 project application form.
- 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 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 must complete the online SecureLab Account Setup form under the SecureLab access step (see further details in Technical Checks).
- 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 to the SecureLab, 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 of SecureLab 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 SecureLab, then you would need to complete and submit a new Agreement.

Whom should I ask to countersign the Agreement at my organisation?

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 ONS data each team member must have Accredited Researcher Status administered by the ONS. 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 ONS 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 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.

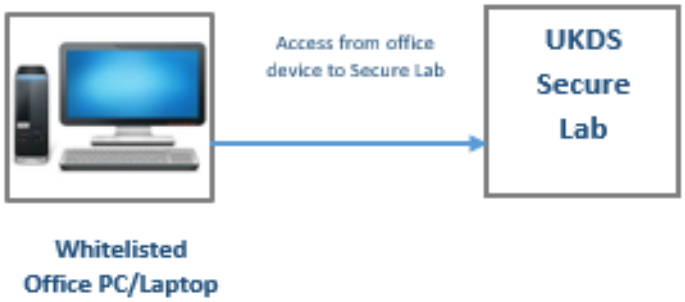
If you completed SURE researcher training with the UK Data Service before 1st January 2019 you will need to complete the SRT course as this is the most up-to-date and relevant SRT course to protect data privacy and required to access SecureLab.

If you have not logged into SecureLab for more than 3 years, you must complete a short online MoodleX refresher course before accessing SecureLab.

Technical checks

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)

Current SecureLab users must complete the form and confirm if the office device has changed when applying for access to a new project.

Please speak to your IT department if you are unsure if your device will meet our requirements.

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
- 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

What happens next

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.

When we are satisfied with the quality of the application it will be sent to the ONS who will review your project.

Applications are usually approved but there are occasions when ONS may have queries, or they may decline the application. In this instance, we will return it to you with feedback to address the queries and then resubmit your application. This is likely to cause additional delays.

Whilst the application is with the ONS for consideration, our Technical Support team will undertake checks on your device and begin setting up your project (and account, if you're not already a SecureLab researcher).

We will confirm the approval decision to you by email. If you have completed all the elements of the application, including attending Safe Researcher training and passed the Technical checks, 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.

Turnaround times can vary as the UK Data Service must apply on your behalf to each data provider and there are additional legislative steps in the process to access controlled data, depending who the data provider is and the access pathway. If the application is well prepared and approval is granted by the data owners with no changes required, you can expect to gain access to the data in approximately 3-4 months, some applications may take longer.

If you require an update on a current application, please email help@ukdataservice.ac.uk, please include your name, institution and the Project ID.

Temporary Home Working Access

Additional measures have been agreed with ONS to enable continued research access to SecureLab throughout the pandemic whilst mitigating risks posed by people working outside their institutional environments. Before applying please check the datasets in your project are approved for home working, a list of current data sets approved for home working access can be found on our website.

In order to access SecureLab projects from home you must connect to your whitelisted office device using a VPN connection from within the UK. The home device must be organisational/institutionally provided. Before applying for access please ensure the criteria below can be met. If you do not have remote access direct to your office device, please speak to your IT support team for assistance. If you require further information please contact techsupport@ukdataservice.ac.uk

Researcher's must apply to ONS for approval to access the project from home and then complete the remaining steps of the home working application with UKDS. All researchers applying for access from home must be named on the ONS application. If you work on more than one project, a separate application must be made for each project.

Apply for ONS approval

Submit a temporary home-working access project proposal to ONS. The form can be downloaded from Download, complete and submit an application to ONS for temporary home-working access and when completed should be emailed to srs.customer.support@ons.gov.uk

Prepare Evidence for technical checks

Gather the following evidence to submit to UKDS:

From your home device - screenshots of the following

- the web page at: https://www.whatismyip.com/my-ip-information/
- for Windows, the output of running the command ipconfig /all in Command Prompt, or for Mac/Linux, the output of running the command ifconfig -a in Terminal
- the operating system and antivirus update status of your device that verify the device is receiving regular updates

From your institution's IT support department

- a description and evidence of your approved VPN - this must include type of VPN; authentication technology used; what kind of measures are in place to prevent and detect unauthorised access attempts, and what measures are in place to check compliance of endpoints connecting to the VPN.
- written confirmation that any information security incidents involving your actions, the VPN, or your office or home PC will be reported to the UK Data Service.

Submit Application to UKDS

When you have approval from ONS and have gathered all of the above evidence please complete the Secure Access additional agreement: COVID-19 temporary home working for ONS data. A full list of the conditions of the agreement can be found at the end of this guide. After completing the agreement please email the evidence to secureforms@ukdataservice.ac.uk.

Notification of Approval

The Data Access team will process the online form and pass the application to the Technical Access team to review the evidence submitted. You will receive notification of home working approval by email.

Conditions for Home Access

Completing the Online Agreement

- Only submit this form when you can agree to all of the following conditions.

- Only use this agreement for **ONS projects that have been approved by the Research Accreditation Panel (RAP), following successful application for home-working access**. If you have not yet applied and received approval for home-working, please do so by following the instructions at https://ukdataservice.ac.uk/covid-19/secure-lab-data-covid-19-update/ons-secure-access-data.
- If your project also accesses Secure Access datasets that are not owned by the ONS (i.e. non-ONS data), you will need to complete an additional non-ONS home-working agreement. This will be checked.
- If you have more than one project that you will access from home (and have been approved to do so), please complete this form for each relevant **approved** project.
- Where indicated, you will need to submit evidence as part of the approval process to: secureforms@ukdataservice.ac.uk. You may not access the SecureLab from home until all the evidence that you have submitted has been checked and approved by the UK Data Service Technical Support team.
- Accessing the SecureLab from home without completing and submitting this form will amount to a breach of the Secure Access User Agreement.
- Access is still restricted to the UK - accessing SecureLab from outside of the UK is not permitted and will constitute a breach of the licence agreement.

Conditions for Access contained in the online home working agreement

- I will access the UK Data Service SecureLab from home under the following conditions, and only where data owners have agreed, and are listed at ukdataservice.ac.uk/covid-19/secure-lab-data-covid-19-update. *I understand that where projects are using data from multiple data owners, all owners and the datasets I wish to use must be listed.*
- I will only use an organisational/institutionally provided computer at home. *Please retain evidence of this.*
- I will only access the SecureLab from home whilst I am in the UK.
- I will use an organisationally/institutionally approved VPN to remotely access my organisational/institutional office computer, and will only access SecureLab through this.
- I confirm that the current Operating Systems of both my organisational/institutional provided (onsite) office computer **and** organisational/institutional provided (home) computer are currently supported by their vendor and have all recommended security updates applied.

- I confirm that the current Operating Systems of both my organisational/institutional provided (onsite) office computer **and** organisational/institutional provided (home) computer have anti-virus software installed and updated.
- While I am remotely connected to my organisational/institutional (onsite) workstation, I will not access anything else on the internet and will close down all other windows and applications.
- I can confirm that I have completed an **information security awareness** training course (e.g. an online institutional course/module such as *Information Security Essentials* through Moodle or Blackboard), **within the past 12 months**. These are usually required to be taken and passed once a year by your institution. *Please keep a record.*
  Please note that any SURE or Safe Researcher training that you have undertaken previously for SecureLab access is not considered to be information security awareness training, for the purposes of this agreement. Please consult your IT team on suitable courses, if you are unsure.
- Please enter the name of the Information Security awareness training course and the date that you completed your Information Security awareness training.
- I will ensure that my monitor is not overlooked by other people in my household when I access SecureLab from home and that my screen will be locked at all times when I am away from my desk.
- If I am using a wireless network to connect to SecureLab at home, it is secured using WPA2 encryption.
- I agree that any information security incidents involving my own actions, the VPN solution, or the home or office PC will be reported to UK Data Service.
- I understand that this is a **temporary service** offered by the UK Data Service and agree that I will stop accessing the SecureLab from home immediately upon cessation of this COVID-19 related service.
- I declare that my institution/organisation has approved me to access SecureLab from home under the same terms of the original Secure Access User Agreement.
- I understand that access to the SecureLab from home without meeting these conditions will constitute a breach of the existing Secure Access User Agreement previously agreed. I understand that any breaches may incur the penalties listed under this existing agreement.

Please see the UK Data Service Privacy Policy for details of how we store and use your personal data.

www.ukdataservice.ac.uk

help@ukdataservice.ac.uk

+44 (0) 1206 872143

We are supported by the Universities of Essex, Manchester, Southampton, Edinburgh, University College London and Jisc. We are funded by UKRI through the Economic and Social Research Council.