UKDS SecureLab user guide

Table of contents

1. An important message

Use of the UKDS SecureLab is based on trust. As a SecureLab user, you trust us to make available an efficient, reliable service with good quality data, and documentation provided by the data owner. You trust that we are on hand to support you when using the SecureLab, and help you with any queries about using the data.

In turn, we trust that you will use the SecureLab in accordance with the terms and conditions specified in the User Agreement. In particular, you will use the SecureLab safely and ensure that the confidentiality of the data is protected.

We understand that undertaking your research in the SecureLab requires a small change in how you work that you may not be used to. This might seem inconvenient – but please remember that you are accessing highly sensitive and confidential data. We believe that a small change in the way you work is a small price to pay for accessing these data from the convenience of your institution.

The SecureLab will continue to evolve. It may be the case that we can improve your experience of using the SecureLab. **If you think that something is unnecessarily inconvenient and could be improved, please tell us** – we may be able to find a way that makes life easier for you but maintains data confidentiality and reassures data owners.

⚠ **Deciding to ignore the rules and procedures outlined in the training course and in this User Guide may well put you in breach of the terms and conditions of use – even worse, it may jeopardise everybody's access to these data.**

If you ever struggle with using the SecureLab, the first action you should take is to contact us:

Email: support@ukdataservice.ac.uk
Helpdesk (9.00 – 17.00): 01206 874968

We are here to help you and make your research possible in a secure environment.

2. The 5 Safes

The 5 Safes Data security model enables us to provide safe access to data that meets the needs of data protection, yet fulfils the demand for open science and transparency.

SAFE DATA — Direct identifiers have been removed, but the risk of re-identification must still be managed

SAFE PROJECTS — Research projects should have valid statistical purpose and a demonstrable public good

SAFE PEOPLE — Educate researchers to use data safely

SAFE SETTINGS — AWS enables access to sensitive data

SAFE OUTPUTS — Statistical Disclosure Control (SDC) is applied to all outputs

Through the combination of these 5 Safes, we can ensure the Safe Use of research data.

3. First steps

3.1. Setting up your environment

As part of applying to access SecureLab your working environment will need to comply with a number of requirements. The setup of your working environment may have already been completed. However, if it has not been completed at this time, or if during the life of your project you move office or institution, your new working environment will need to be assessed as follows:

Technical requirements

- The Registered User must ensure adherence to technical requirements for accessing SecureLab, liaising with their organisation as necessary and providing necessary information for device and environment checks as requested by the Data Service Provider.
- The Registered User is responsible for ensuring that the device used for SecureLab access is either managed by their institution or a designated third party on behalf of their institution. The use of personal devices for SecureLab access is strictly prohibited.
- The Registered User must ensure that the device used for SecureLab is connected to the internet either via a wired Ethernet connection or WPA2/3 encrypted wireless connection managed by the host organisation.
- The Registered User is responsible for ensuring that only the network interface used for SecureLab access is active and that the device does not run services allowing third-party connections, such as web servers or email servers.
- The Registered User must ensure that no screen capture tools are running on the device during SecureLab access.

The following security measures must also be observed:

- When SecureLab is accessed, only the wired Ethernet is used, and that the wireless is not connected simultaneously.
- The user only accesses SecureLab from their designated office, not from any other location on or off campus.
- That good security measures are observed by the user, for example locking screens when leaving unattended, not allowing screens to be visible to people other than SecureLab users working on the same SecureLab project.
- The user's SecureLab credentials are not saved in the web browser.
- No other applications, particularly web based ones, are running whilst SecureLab is being accessed.
- If the layout of your room/workspace changes substantively you must notify the SecureLab Helpdesk immediately and not use the service until authorised to do so.
- A privacy filter must be fitted if there is a chance that your screen will be overlooked.

In addition to this, please also attach screenshots of the following:

- For Windows PCs - the output of running the command "ipconfig /all" in Command Prompt.
- For Mac/Linux - the output of running the command "ifconfig -a" in Terminal.
- The web page at What's My IP.

4. Logging on

4.1. Getting started

Before you can begin using your SecureLab account, we will require a screenshot of your IP address details.

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.

4.2. Anti-virus and anti-malware software

One of the conditions of using the SecureLab is that the computer that you are using has appropriate anti-virus and anti-malware software installed. Please ensure that you have such software installed on your computer, and that it is up-to-date at all times. For help, you might need to speak to your institution's IT support.

4.3. Username and password

Remember to keep this password safe – don't write it down or share it with anyone else including other members of your project team and the UK Data Service support team.

If you forget your password, you can request a new password by completing a 'Website/technical issue' online form.

4.4. Logging on

You can log into your SecureLab account via the UK Data Service website.

Just click on the 'Register / Login' button in the top right corner.

(For a refresher, you can review our How to log in to UKDS SecureLab video by navigating to YouTube.)

Then choose the 'Login to SecureLab' link for approved researchers:

You will now see a pop-up reminding you that if you are to proceed, that you agree to abide by all clauses of the Secure Access Agreement, and that you are accessing from the approved location declared in your application.

If you agree, please click 'OK – I agree'.

Once the page has loaded, you'll be asked to enter your SecureLab username and password. We have implemented Multi-Factor Authentication (MFA) for extra security, so you will also be asked for a password token. If you don't have a password token, please click 'Don't have a token?'

In order to generate a token, you will need an Authenticator App on your smartphone. There are a number of providers of free MFA apps that you can use with SecureLab. These include Microsoft Authenticator and Google Authenticator. Please note that the UK Data Service does not have an official affiliation with these apps, and encourages you to choose an MFA solution that works best for your device.

To register a token device, you first need to verify your identity. Enter your username below to send an email with a verification code.

Username

domain\user or user@domain.com

Next

Cancel

Please enter your username and click 'Next'. It may take a minute or two but you will be emailed a Verification Code. Please remember that your email; address must be institutional, NOT hotmail, gmail etc.
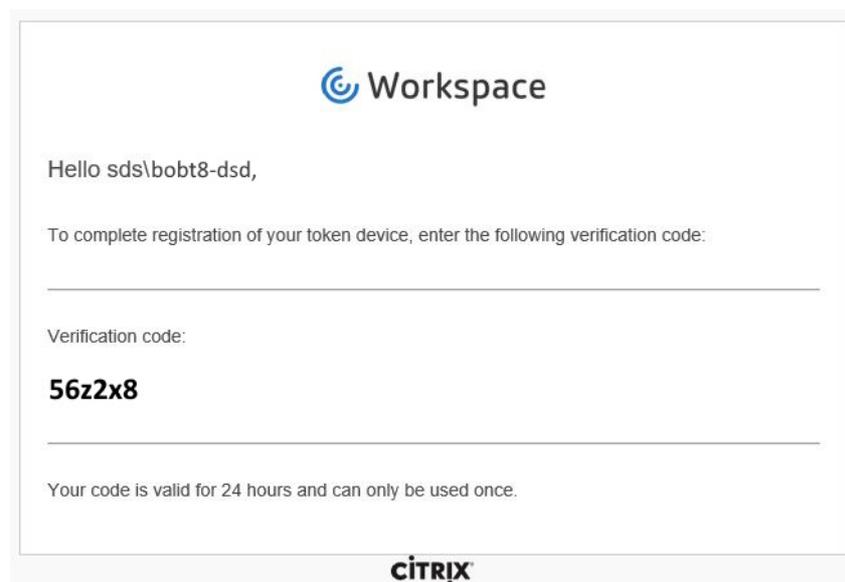
Once you've entered the Verification Code you'll be taken to a page with a QR Code. Please open your previously downloaded Authenticator App on your phone, and scan the QR Code. This will register your device.
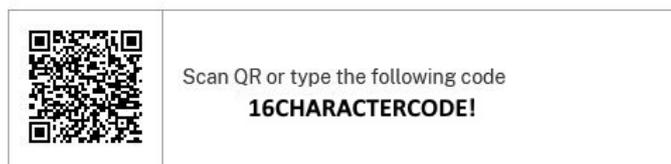
You should only need to register your device the first time, so you will be able to skip this step for subsequent SecureLab sessions. Click 'Finish and Sign In'.

On the next page, enter your Username, Password, and Password Token. Your Username and Password will have been provided to you after you have passed the test which is part of the compulsory training. Your Password Token is the 6 digit code you will see on your phone's Authenticator App. This changes every 30 seconds.

The screen below should appear. Click on the 'SecureLab' icon to access your account.
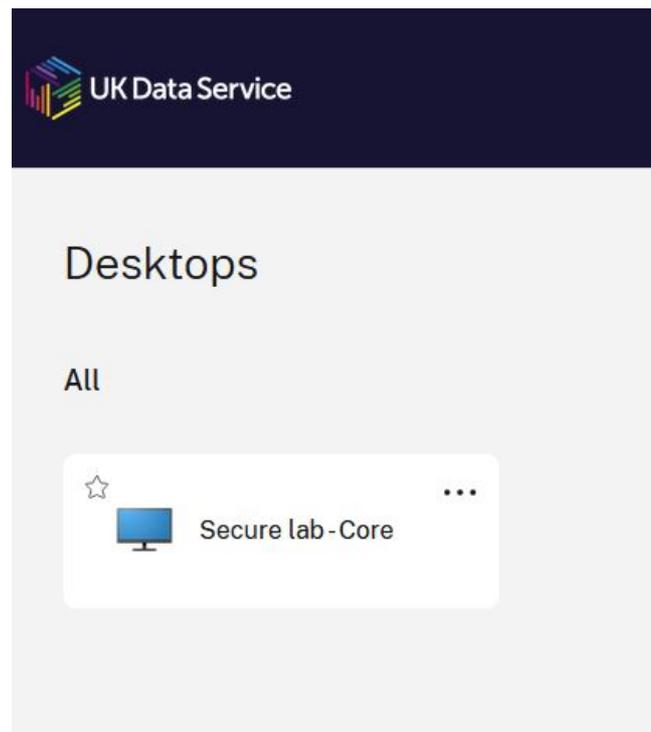
⚠ **Do not double click** on the 'SecureLab' icon as this may open up two sessions which will cause problems later.

A window will then appear which tells you that your account is launching.
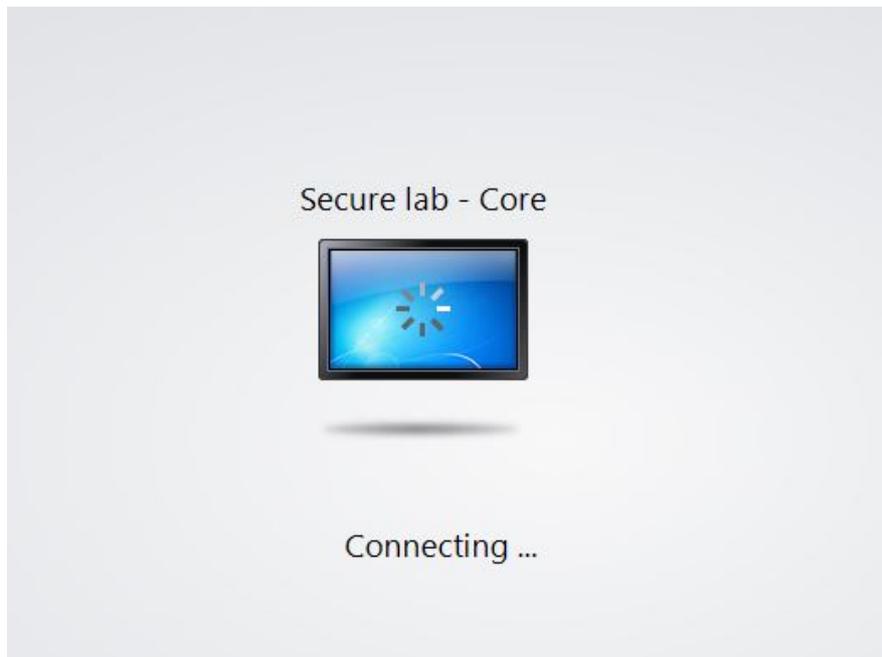
After a few seconds, a standard Windows desktop will appear.

Note that after five minutes of inactivity, you will be asked to re-enter your password to access your account.

You will also notice a message that reminds you that your SecureLab session is recorded for security purposes and that **SecureLab is unavailable every Tuesday between 10.00 and 12.00.** Please click 'OK'.
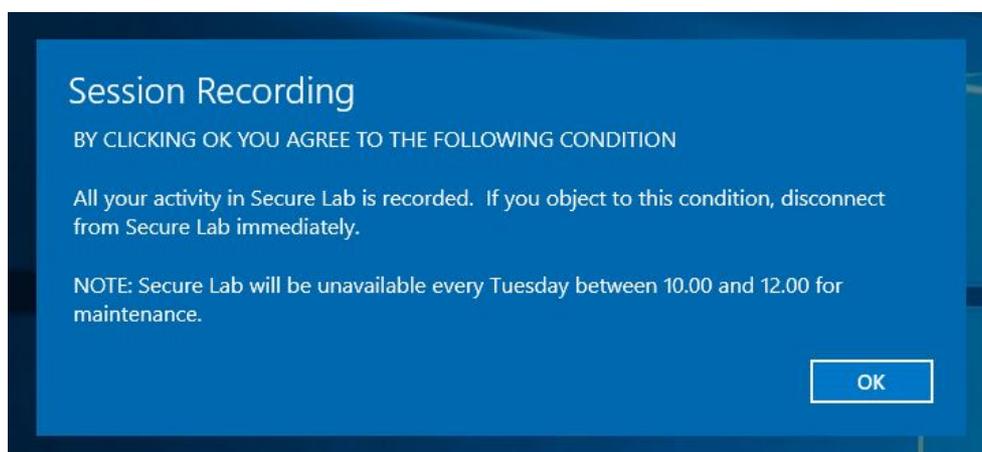
Now click on 'File Explorer'.

(Please note that if you don't have the window at full size you might only see the blue desktop background; set window to full size to see the start button).

You are now logged on.

You should make a note of the login URL in case for some reason the web page is unavailable: secureaccess.ukdataservice.ac.uk/

5. Logging off

It is really important that you log off from the SecureLab properly; otherwise you might experience future connection problems.

To log off properly, go to the 'Start' Menu in the bottom left of the screen, click the 'Power' icon and select 'Disconnect'.
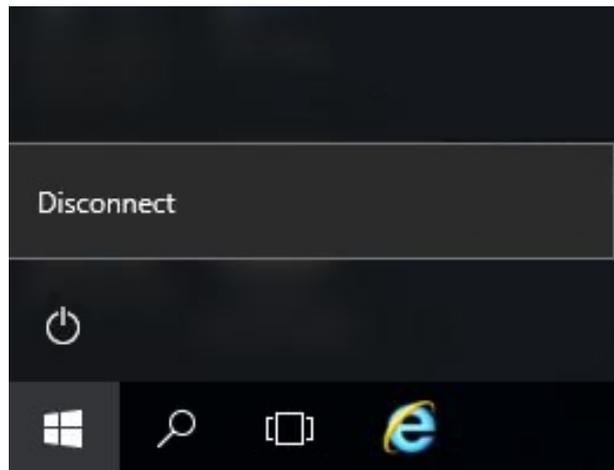
If you wish to leave a program running (for example a Stata program that takes a few hours to run) you may do so. You should just Click 'Disconnect' from the dropdown menu at the top centre of the screen. You will still be logged on, and your program will be running. To return, just log back into the SecureLab using the normal method (see previous section).
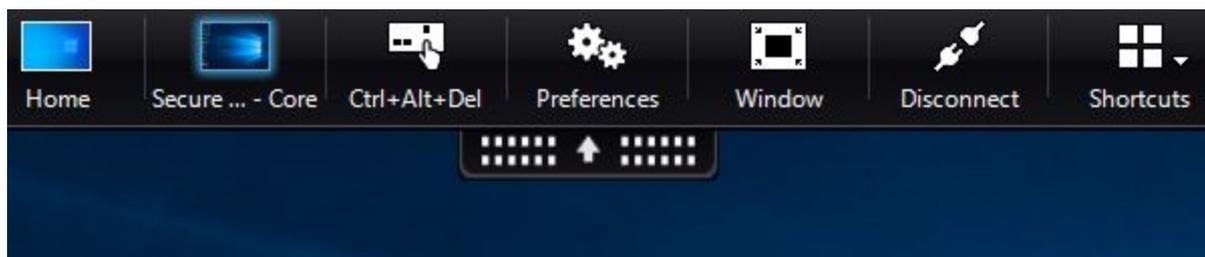
But if you have finished your session please log off – otherwise you are taking up somebody else's SecureLab space.

Please be warned however, that while you leave a session running unattended, there is always the possibility of a network error at our end or your end, which could interrupt the session. Also be mindful of the interruption caused by the Tuesday maintenance session (see Section 18.1).

6. Your SecureLab account

Once you have successfully logged on, you can click on 'File Explorer'. You will see the following two drives:
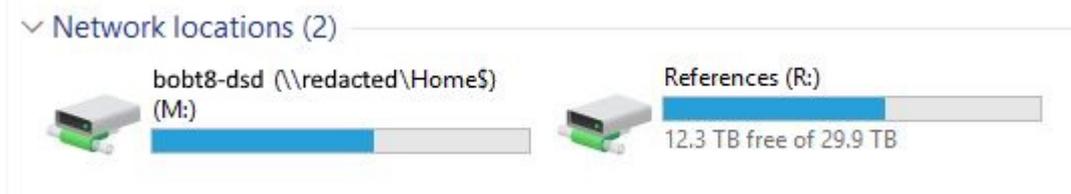
6.1.   Your M: drive

Inside your M: drive, you'll find a project folder for each project that you are registered to undertake using the SecureLab. In turn, each project folder contains the five folders pictured in the screenshot below. You cannot change this folder structure.
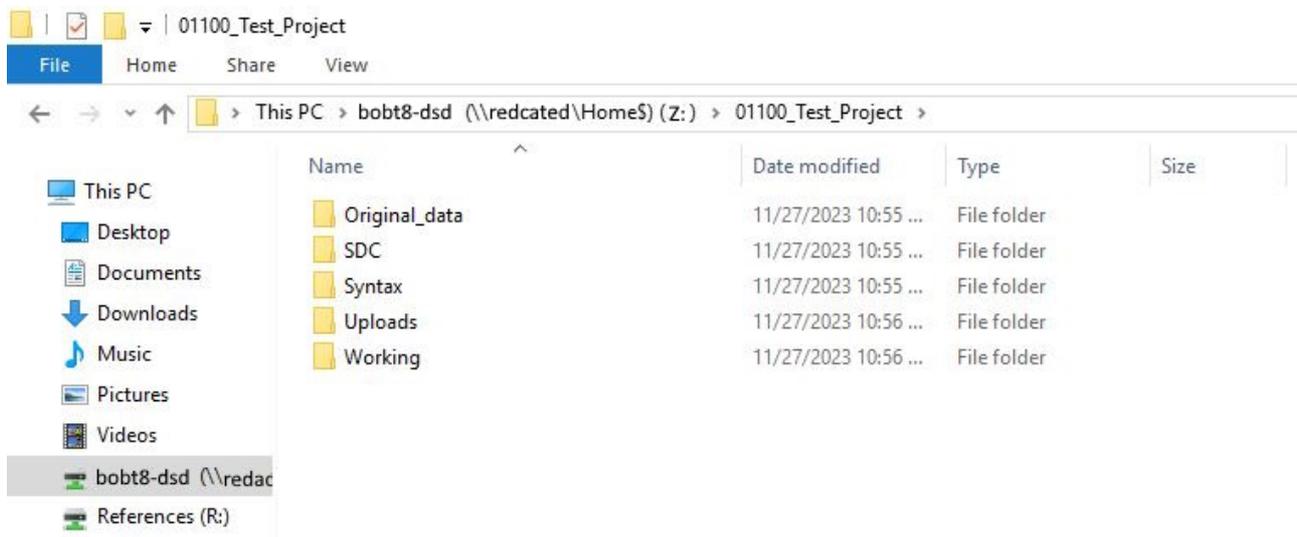
6.2.   Original_data folder

Here's where you'll find the data for each project that you have applied to access.

Each dataset will be stored in its own dissemination pack (for example, 6644_ARD):
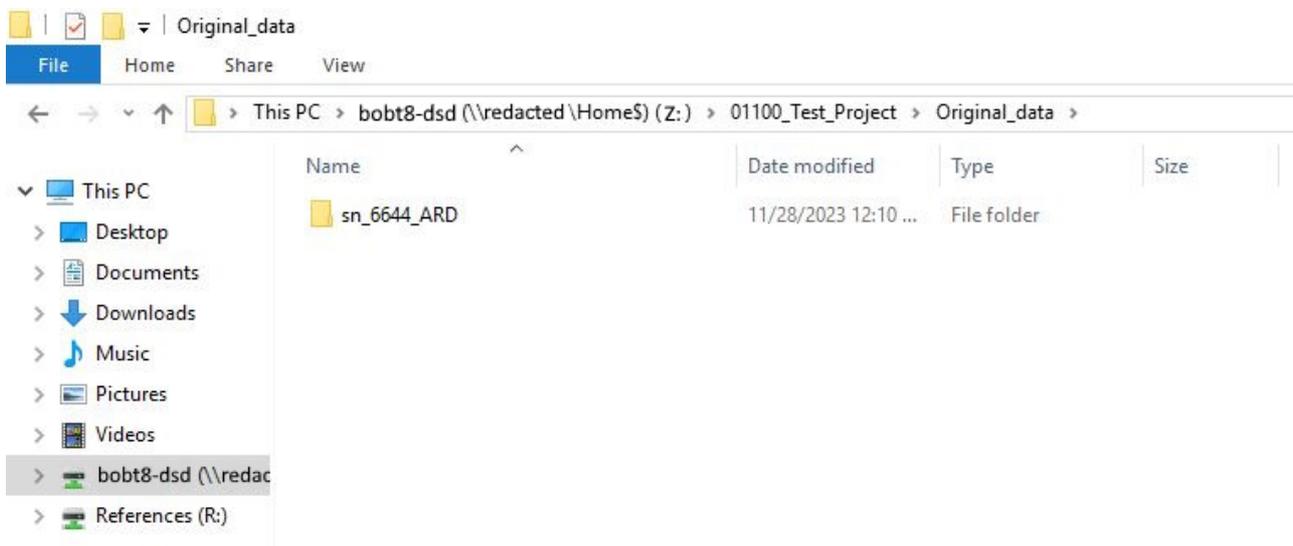
This is useful if you have applied to use more than one source of data for your project. Note, this is a 'read only' area – you cannot overwrite any files saved in the 'Original_data' folder. This ensures that you always have a 'clean' copy of the data.

6.3.   Statistical Disclosure Control (SDC) folder

When you have completed your project and you would like the UK Data Service team to release your work to you, save your files to the 'SDC' folder (for more information on this, see Section 14 "Requesting outputs").

6.4.   Syntax folder

We recommend that you keep all of your syntax files in this folder.

It is important to note that after you have finished your project, **we will only keep files that have been saved in the Syntax folder**. We cannot store data files for all our users as this would become expensive for us. Instead, we encourage our users to write good syntax that can easily recreate data files in the future.

Also, if you accidentally delete a data file, you can use your syntax to recreate it (although we can recover deleted files, there may be some delay). The Syntax folder is the place to store these finished and cleaned syntax files.

6.5.   Working folder

Your Working folder is your project working area. You can use this folder to save data files that you are manipulating, drafts of papers, presentations and other outputs, draft results of your analysis, etc.

6.6.   Uploads folder

If you ask us to upload any files to your SecureLab account (e.g. syntax that you have written at home, background information, or external data), we will save the files here, in the Uploads Folder. However, please note that this is a 'read only' folder.

Some publicly available files are exempt from the upload process, because they might be relevant to other SecureLab users too. Such files will be placed in the References drive (see Section 6.8). We will let you know if a file you requested has been already uploaded to this drive.

6.7.   Important: please remember

Do not save files onto your desktop: if you do, they may not be available the next time you log on.

The UK Data Service operates the SecureLab with a 'Fair Usage Policy'. This states that, if the size or number of files that you generate impacts on other users or the overall system performance; we reserve the right to request that you remove files, or the UK Data Service team can delete files.

6.8.   References (R:)

In this drive you'll find reference files. The reference files contain useful information for all researchers to access. For example, the References drive contains:

- the National Statistics Postcode Directory
- Standard Occupational Classification codes
- Standard Industrial Classification codes
- geographical lookup tables
- User Guides.

You will also find a folder called 'ADO_Files'. This folder contains ADO files for Stata users. If you need to run an ADO file you cannot do this in the usual way as the SecureLab has no internet connectivity; however, you can run them from this folder instead.

Enter the following command into Stata to set the ado path directory:

```
adopath ++ R:\ADO_Files\
```

This will enable you to subsequently call the ado files stored on the references drive.

If you require an ADO file that is not yet available in the 'ADO_Files' folder, please email us and we will add it for you. **Please remember to check the 'ADO_Files' folder before you make a request.**

To install R packages in SecureLab, please follow the Guide on 'Using the local R Repository on Secure Lab' which can be found in the SecureLab folder 'References$\User_Guides\Guide to working with R packages in the SecureLab'.

6.9.   Applications (Desktop)

On your SecureLab desktop you can find the analytical and word processing software you need to carry out your work.

These include Stata, SPSS, R and Microsoft Office amongst others (visit our webpage for a full list of software available on SecureLab). If there are applications that you would like to use, but can't see, please speak to a member of staff at the UK Data Service, and we might be able to install these for you.

6.10.   SPSS functionality

Researchers who intend to use SPSS in the SecureLab should note that we have the Premium Subscription of SPSS available.

We have the following SPSS licences in SecureLab:

- Statistics
- Regression
- Advanced Statistics
- Categories
- Exact Tests
- Missing Values
- Conjoint
- Custom Tables
- Complex Samples
- Decision Trees
- Data Preparation
- Forecasting
- Neural Networks
- Direct Marketing
- Bootstrapping
- Statistics Base.

If other functions are crucial for the research, we advise researchers to switch to Stata, Mplus, Python or R to run their analyses. This will allow researchers to continue with their research.

7. Dissemination packages

Each dataset that the UK Data Service provides access to in the SecureLab comes in a 'Dissemination Package'. This is the folder in the 'Original_data' folder with the study number, name of the dataset and the date when the data were received from the data owner (e.g. 6340_BHPS_4th_Ed_Oct18). When you open up this folder, you'll see something similar to this:

📁 mrdoc	12/03/2012 16:41	File folder
📁 stata	12/03/2012 16:41	File folder
📝 6340_file_information	04/02/2011 06:50	Rich Text Format
read6340	03/02/2011 11:17	HTML Document
UKDA_Study_6340_Information	04/02/2011 07:02	HTML Document

The 'mrdoc' folder contains all available documentation for the dataset. The documentation varies from one dataset to another, but generally includes the survey questionnaires and a user guide. It also includes a 'Data Dictionary' - this is a complete list of all variables and label values within each data file.

Documentation for each SecureLab dataset is provided by the relevant data owner. Part of the remit of the UK Data Service is to improve the quality of documentation, which is an on-going process. For example, you'll find miscellaneous documentation compiled into bookmarked pdf files for easy searching of queries and terms.

The data files are contained in the folder with the name of the data format. In the example above, you'll find all the data files in the 'Stata' folder and the files will be in Stata format (if you asked for another format other than the one you see, call us and we'll replace it).

The Word document with 'file information' is useful because it provides a complete list and brief description of all data and documentation files contained within the dissemination package. This allows you to search for types of data, or available documentation, in a convenient place.

Before you begin using the data, have a look through the 'read' file. This contains important data processing notes, and will include any data quality issues that we have identified when processing the data.

You will find the 'Study information' file ('UKDA_Study_xxxx_Information') useful because it contains the correct data citation and acknowledgement statements that you should include when you are publishing your work. The 'Study information' file also contains all the information that is available in the online Data catalogue record for the study, including sampling frame details and topics covered in the data.

7.1. Data revisions and new editions

A **new edition** of a dataset is made available when a new time period has been covered by the study, or reweighted data have been received from the data owner, and are ready for us to make available to researchers. For example, if the latest quarter of the Labour Force Survey is ready, we will create a new edition of the 'Dissemination Package' that will include this new quarter. We will automatically deposit each new edition into your project when it's ready and will notify users via email. New editions will be contained in a folder named with the edition number (e.g., 6697_BSD_15th_Ed_Feb23)

Sometimes data will be **revised**, for example as a result of a quality improvement, or amendment of a previous error. In this case, we will create a revised dissemination package, and add this to your project in a folder named with the word 'Update' (for example 6697_BSD_15th_Ed_Feb23_Update). New researchers will only receive the most recent revision. However, we will archive previous editions in case any researchers require older versions.

8. Working on multiple projects

There is no limit on the number of projects that you can apply to undertake in the SecureLab. Users will often be engaged in several projects at a time. As you become familiar with the SecureLab setting, we hope you will consider applying to use more of the data that we can provide access to. If you wish to use the data you are already using in SecureLab for a different research purpose you will need to apply to set up a new project – remember, you have been granted access to that data for the specific purpose you outlined in your original research proposal only.

Working on multiple projects should be straightforward. As you apply for data to undertake additional projects, you will find that a new project folder will appear in your user account.

Name	Date modified	Type	Size
R_Library	9/23/2021 1:07 PM	File folder	
WINDOWS	4/15/2019 12:00 PM	File folder	
12345_Test_Project	9/27/2021 12:26 PM	Shortcut	2 KB
123456_Test_Project	9/27/2021 12:26 PM	Shortcut	2 KB

In this example, you'll see a folder for each of two current projects.

Each folder will be set up, as explained in section 6 'Your SecureLab account'.

When you make an output, or import, request, Please ensure that you provide the correct project number. **You must not attempt to copy files of any sort from one project area to another as this would constitute a breach of your secure access agreement**.

8.1. Using a syntax file for more than one project

If you have created a syntax file in one of your projects that you would like to use in another of your projects, please let us know and we can upload this into the second project for you.

9. Permission to use data

Please be warned: You should only use data for a project that you have permission to use. If you want to use a derived dataset for a new project, you must apply to use the data that generates the derived dataset.

If we review an output and we find that you have used data – derived or otherwise – that you have not been approved to use for that project, we will not be able to send you your output, and there may be additional penalties.

Applying to use additional data sources is simple. For details, see Section 12 'Applying to use additional data'. Remember; always talk to us if you need advice. If you require additional data to be added to your project, we can help arrange permission.

9.1. Project expiration dates

When you are working on more than one project, you should be aware that one project is likely to expire before another. Our Access team will contact you prior to any of your projects expiring, to see whether or not you need an extension to the project.

10. Working with team members

The SecureLab has been designed so that researchers can easily work together on the same project.

Please note that **all** researchers who wish to access data or results within the SecureLab environment must apply for access, and therefore must be Approved Researchers or Accredited Researchers.

All researchers working on a project will be provided with their own username and password (as they are each provided with a SecureLab account). Researchers that work on a joint SecureLab project must not share their usernames and passwords with each other. Each researcher should only access the project with their own user account.

For example, when two researchers are working on the same project, both will see the project folder relating to their joint project. This is illustrated in the diagram below.
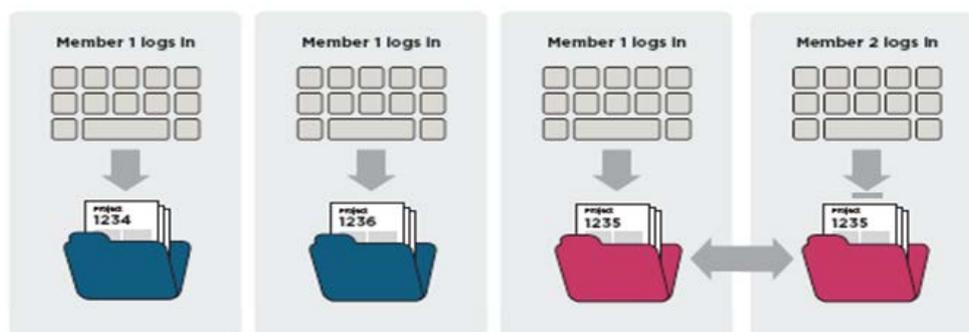
In this example when Member 2 logs on, they will only be able to access one project folder (Project 1235), which they can work on collaboratively with Member 1. They cannot see the other projects Member 1 is working on.

If either member creates a file and saves it in this folder, then the other member will be able to access it. Therefore, results can be shared.

It is also possible for both members to open up the same file. This is useful if they wish to discuss their results over the telephone. However, researchers should not discuss the details of the project with people outside of the project team.

10.1.   ESRC Associate Researchers

If you are working with a researcher using ESRC, or other non-ONS data, in SecureLab, but you do not need to work with the data yourself (the most common example of this is a PhD supervisor), you may take the Associate Researcher online training course. Passing this short online course entitles a PhD supervisor (for instance) to look at results on the researchers' screen, which may be useful for discussion, but **they must not look at the data**. Again, the researcher must not share their password with the Associate Researcher.

10.2.   If you wish to add to a new, or existing, researcher to your project

Project Leads can add additional researchers to their project record via their UK Data Service account. The additional researcher(s) will need to be registered with the UK Data Service before they can be added to a project, and the Project Lead must ensure that the email address they use to add the additional researcher matches the email address on the researcher's account.

If the additional researcher is not registered, or has a different email address on their account to the one the Project Lead is using to add them, then the addition in the system will be unsuccessful.

Once the Project Lead has added the new researcher to the project record, they will then need to go through the relevant approval process for arranging access to the SecureLab

project area. The process varies by dataset, so the Project Lead should email our Helpdesk for specific guidance.

11. Importing your documents, data, syntax and programme extensions

We have made importing data, syntax, documents and programme extensions as easy as possible for our users.

11.1. Importing data into your account

This section applies to data not available from the UK Data Service collection. To learn more about how to add UK Data Service data, see Section 12 'Applying to use additional data'.

Please remember that in some cases, if you wish to bring in data that is not hosted by the UK Data Service to use in conjunction with data available via your SecureLab account, we may be obliged to seek permission from the owners of the Secure Access data.

If you wish to import data into your account, please complete a 'Request to Import Data' form, by navigating to UK Data Service.

This form asks you to provide:

- general information about the data you wish to import
- names of the data files
- variable names and variable descriptions
- why you require the data for your research (for example, how they complement the data you have applied to use through the SecureLab)
- evidence that you have permission to use the requested data in the SecureLab (see sections 6 and 7 of the form).

Please send the form and evidence to us using the University of Essex's ZendTo Service. Where appropriate, we will forward the form to the data owner for approval.

11.2. Sending us your data

Your request will be reviewed by the UK Data Service and, where necessary, the relevant data owners. If your request is successful we will ask you to send your dataset.

All data should be sent using our University of Essex's ZendTo Service. ZendTo is a drop-box style online server, which allows you to upload files. You can submit up to 2GB of files in a single request. When you have uploaded your files, a notification is sent to our Helpdesk, and a User Support Officer will transfer the files to your account.

If your files contain any microdata you must use encryption software, e.g. VeraCrypt (navigate to VeraCrypt to encrypt files first) Our YouTube video 'How to create an encrypted volume using VeraCrypt' explains the process. We also allow 7Zip (but not WinZip).The encrypted folder with the microdata should then be sent via the University of Essex ZendTo Service (see below), not as an email attachment.

Please scan your files for viruses or malware before sending them to us.

The same 'Request to Import Data' form mentioned above can be used if you wish to add data to your account after you have been approved. However, depending on the source of the data, we may still be obliged to seek permission from the Secure Access data owner.

Here is a step-by-step guide:

1. We will pass your completed 'Request to Import Data' form to the data owner to obtain their permission (if necessary).
2. You will receive an email confirmation from us when permission has been granted.
3. We will add your data to your SecureLab account. The data will appear in the 'Uploads' folder inside the relevant project folder. (For details, see section 6 'Your SecureLab account').

Please remember that all files will have to be screened by us for viruses, malware etc. before we can deposit the data in your SecureLab account.

11.3.   Importing syntax into your account

If you have created your own syntax file (for example, a Stata file or SPSS syntax file) and you would like this to be available in your SecureLab account:

1. Send the syntax file to us using the University of Essex's ZendTo Service.
2. Please remember to include your name and project number (so we can save the file in the correct location).

We will check your syntax file(s) for viruses and carry out a content check to ensure no data are included.

We will place the syntax files inside the 'Uploads' folder, within the relevant project folder and notify you when this has been done.

11.4. Importing Word document into your account

If you have written part of your future paper, such as the literature review, study aims or methodology, in Word outside of SecureLab and you would like this to be available in your SecureLab account:

- Send the Word file to us using the University of Essex ZendTo Service. Please remember to include your **name** and **project** number. (This will ensure we save the file in the correct location.)

We will place the Word file(s) inside the 'Uploads' folder, within the relevant project Folder, and notify you when this has been done.

11.5. Importing programme extensions into your account

If you require programme extensions that are *not currently available* in the references drive to be available in your SecureLab account:

11.5.1. Stata ADO files

In the case of ADO files you should check the 'ADO_Files' folder in SecureLabs' References (R:) drive. If the ADO file you require is not already supplied in the 'ADO_Files' folder please email support@ukdataservice.ac.uk to request the ADO file you need. We will download the file from the SSC (Statistical Software Components) website and, once a virus check and content check have been performed we will add the ADO file to the 'ADO_Files' folder and email you to let you know it is available.

For guidance on how to use ADO files from the 'ADO_Files' folder, please read the '!1.Setting Stata path directory for ado files' document, which is in the same location.

11.5.2. R files

We have a weekly updated local repository for R packages, which mirrors CRAN, on the Reference drive on UKDS SecureLab. To install packages from there, please follow the instructions in the SecureLab folder 'References$\User_Guide\Guide to working with R packages in SecureLab.

It is possible to request the import of packages that are not on CRAN. However, the process is much slower, as we have to check these packages one-by-one to ensure that no malicious code or data is included. Each request will be processed on a case-by-case basis, and we will require you to explain why you need the package, and provide relevant documentation and citation. Please email us at support@ukdataservice.ac.uk if you require such a package.

Please remember to include **your name** and **project number**. (This will ensure we save the file in the correct location.)

12. Applying to use additional data

You may have started your project and realised that you need to use data from other sources. This section helps you apply to use sources of data in addition to those sources in your original application.

12.1. If you're not sure what data you need

Please contact the UK Data Service team. We are happy to advise you about data that can assist you with your project. Alternatively, use our Data Catalogue to search for related data by navigating to UK Data Service.

12.2. To apply for additional Secure Access data

Request our 'Additional Data' form, available from secure.applications@ukdataservice.ac.uk and return to us.

On this form, you will need to explain how the additional data will benefit your research project.

We will then forward this form to the data owner, and once the request has been approved, we will add the new data to the relevant project folder in your account.

12.3. If you wish to use data available through other licences

You may wish to use data available through the 'End User' or 'Special Licence' agreements. Details about these data, and how to apply for them, can be found on the UK Data Service help section.

13. Linking external business data to ONS business data

13.1. IDBR matching

The IDBR (Inter-Departmental Business Register) team at ONS offers a matching service whereby the IDBR reference can be matched on to data containing the CRN (Companies House reference numbers) and/or other identifiers.

Please remember that if you wish to link external business data to data available via your SecureLab account, permission must be granted from the external business data owner (e.g. Growth Intelligence) and the Secure Access data owner (ONS). If the linking was not specified in your original project proposal the Service can contact ONS to request permission.

13.2. How it works

If you have Companies House or FAME data containing CRNs the IDBR reference number/s for that company can be matched onto your dataset. This is achieved through a CRN to IDBR reference number lookup table **held by ONS**. This table is not available to researchers because it is quite easy to look up the name of a company on the Companies House website using the CRNs, so once these are linked to the ONS business data, there would be a greater risk of breaching confidentiality than is deemed acceptable. However, it is possible to have data containing CRNs linked to the IDBR reference numbers by ONS, who will then make available the resulting data file without the CRNs included. You can then match the file to the ONS business data you are using.

The IDBR structure and 'enterprise' variable[1]

Enterprise Group	Small Motors
Enterprise	Small Motors Ltd
Local Units	Small Motors Newport / Small Motors Cardiff
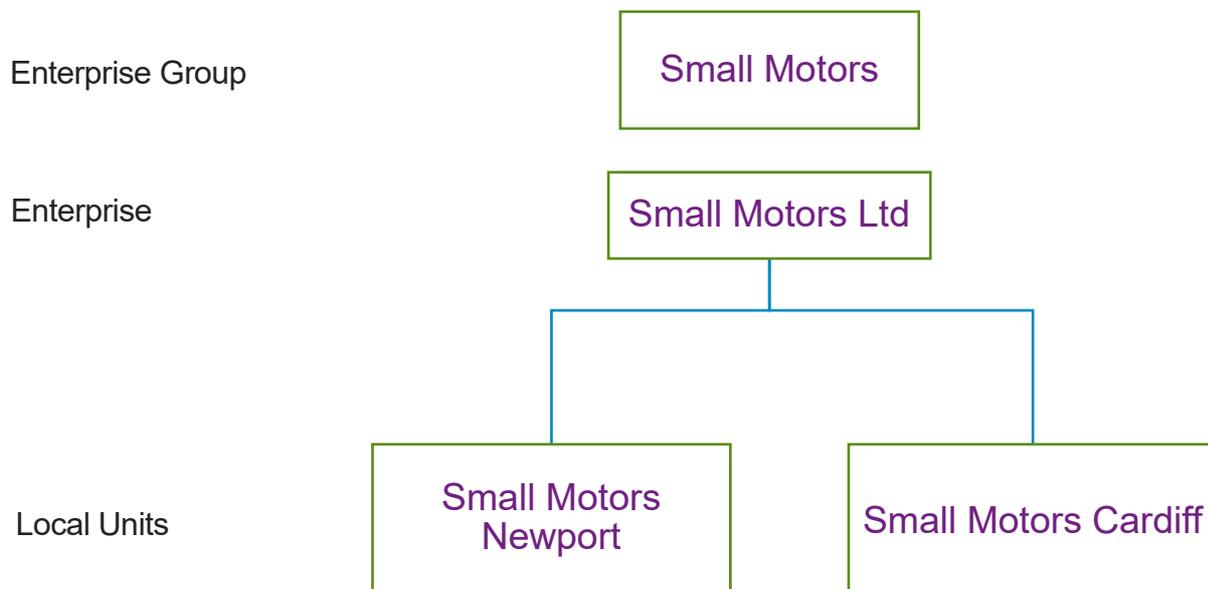
The 'enterprise' can be thought of as the 'company'. Local units are 'plants', for example, a retail outlet or factory. The plant is the source of business activity. It may be a factory that produces finished goods or an accountancy office. The example above shows an enterprise group which owns one company 'Small Motors Ltd'. This company controls two local units: 'Small Motors Newport' and 'Small Motors Cardiff'.

---

[1] Adapted from Evans, P. and Welpton, R. (2009) Business Structure Database: The Inter-Departmental Business Register (IDBR) for Research. Economic & Labour Market Review. 3 (6), 71-75.

The CRN-IDBR lookup table contains the **enterprise** reference. Note that the mapping is not one-to-one: some CRNs map to more than one enterprise and some enterprises to more than one CRN.

13.3.   I would like ONS to carry out the linking, what do I do?

The IDBR team at ONS offers a matching service whereby the IDBR reference can be matched on to data containing the CRN and/or other identifiers (e.g. VAT reference, PAYE reference, Companies House name). The IDBR team make a charge for this service.

If you wish to commission linking work from the IDBR team, we can arrange this. We will transfer your dataset to ONS and then, once the linking work is complete, into your SecureLab account.

To request assistance this service:

1. Please complete the 'SecureLab import data request' form, by navigating to UK Data Service.
2. Under section 3 please indicate the type of assistance you require (e.g. I will be commissioning the IDBR team to conduct the linking and require UK Data Service to transfer the files).
3. Please complete and return the form to the Support Helpdesk using the University of Essex's ZendTo Service with the following information:
   Evidence that you have permission to use these external data in the SecureLab, for example, by attaching any email correspondence confirming permission.
4. We may contact you to discuss the linking and if required we will forward the form to the data owners for approval.
5. We will contact the ONS to arrange for the linking to be undertaken, and will copy you into the email correspondence. ONS can then liaise with you to agree the work and arrange payment.
6. We will send you instructions for sending your data, if following appropriate review by the Service (and relevant data owners where necessary), your request has been successful.
7. Once we have received the matched data from the IDBR team, we will place it in your 'Uploads' folder.

13.4. Preparation and turnaround

ONS will advise on linking commissioned from the IDBR team and will advise you on the required data format.

14. Requesting outputs

As you learned during the training course you attended, in order to keep data secure, it is not possible for users to remove any files from our SecureLab servers.

We also examine your statistical outputs to ensure that they cannot be used by anybody to identify an individual or organisation from the data you have used (known as Statistical Disclosure Control).

14.1. What is an output?

By 'outputs' we mean statistical results that have been written up for publication and/or presentation in Word or LaTeX will have selected the results you wish to present to the outside world, from the analysis you have generated inside the SecureLab, and written up the results. The output should be of a 'publishable quality' and have a specific purpose/use. It is possible for us to release csv files in exceptional circumstances. However, they take longer to check – especially where there are a several files - and our five working days turnaround is likely to be exceeded. You must still provide sufficient contextual/analytical explanation.

Publishable outputs include written documents and presentations. The publishable output types that are permitted for release from the SecureLab are:

- journal publication/paper
- working paper
- book chapter/book
- commissioned/policy report
- report to funder
- final report
- interim report
- conference/seminar presentation (not in PowerPoint – see in section 14.8 'Points to remember when submitting output requests')
- research dissertation/thesis/chapter.

You should also ensure that your output meets our minimum requirements (see section 14.8 'Points to remember when submitting output requests').

We recognise that outputs will not always be 'final' and that you may wish to carry out additional analysis inside the SecureLab, for example, in response to comments from a journal or funder, and submit a revised output for checking. We are happy to check revised outputs, however, you should ensure that your output is finalised as far as possible before submitting it for checking.

Researchers must produce their output(s) inside the SecureLab. If you wish to import textual information into the SecureLab – i.e. written information such as literature review, study aims etc. that can be written without looking at the data – in order to compile a publishable output then you can send this to us. See section 11 'Importing your documents, data, syntax, and programme extensions' for guidance on how to do this.

14.2.   Intermediate results

We will not release results to researchers if they are not of a 'publishable quality'. For example, we will not release a Word document containing many tables and graphs, with some basic information (e.g. dataset used, sample), but no clear selection of results and/or write up of the results, as we would expect from a publishable output. Nor will we release one small table.

The above are examples of what we call 'intermediate' results. We do not release such results to users – only publishable outputs, as explained above.

A rule of thumb for remembering this is to ask yourself **"What would I submit to a journal or funder?"** or **"What would I present to a conference?"** Clearly, you wouldn't submit numerous tables or graphs to a journal, with no clear write up of the results. Nor would you submit one individual table.

If you are unsure of what you can request, please contact us. We're happy to answer your questions.

14.3.   Why do we only release publishable outputs?

When undertaking Statistical Disclosure Control of outputs, it is important that we are able to view the results in context. Reading the text that explains the results in a publishable output helps us to make a quick, and fully informed, decision about whether the output is suitable for release. If we undertook Statistical Disclosure Control of intermediate outputs, we would have to contact you and ask you to explain the context and meaning for each set of results. This would be tedious for you and slow down the process of releasing outputs to you.

The Support Team is a small team of dedicated professionals who have responsibility for many support tasks. Statistical Disclosure Control is a manual task carried out by two

independent checkers and is thus a time-consuming activity. Releasing intermediate outputs would increase the workload to an unsustainable level.

In addition, intermediate outputs tend to include a larger number of tables; this increases risk of secondary disclosure within the document. Releasing intermediate outputs would also result in a larger number of total output requests per project hence increasing risk of secondary disclosure across different output releases. We cannot check across different outputs.

There should be no need for us to release intermediate outputs. If each researcher on the team has a SecureLab account, they can log on to their account to see the results produced by their colleagues. We also ask PhD supervisors to become Approved/Accredited Users so that they can also have a SecureLab account, and can view their student's results within the secure environment, and recommend any changes to the work that need to be made. However, if a project colleague is not based in the UK (which means they cannot have access to the SecureLab) we may consider releasing intermediate results. You should contact us to discuss the situation.

It is also easier to clear publishable results as it is easier to understand what the results tell us, and we can return the results to you more rapidly.

14.4. Before you submit your output

We cannot release your output unless we are happy that the risk of re-identification of an entity is so low as to be virtually non-existent. If we have to contact you for clarification, this will cause delays. To increase your chances of having your output released at the first statistical disclosure check, you should use the following as a checklist:

General

We recommend that you allow 24 hours between finishing an output and submitting the output request form to us; this gives you a little time to reflect on the output and ensure it needs no further work before submission.

Researchers can submit one output request at a time. This means that **you cannot submit a new output request until your original one is concluded** – any new output requests made prior to your original output request being concluded will not be processed. We do not release Microsoft Excel files or PowerPoint files for security reasons.

Rules of Thumb

As part of the training course you attended, you will have been given a comprehensive account of the 'rules of thumb'. Before you submit your output to us for statistical disclosure checking please ensure that your output complies – *and clearly demonstrates that it complies* - with the following:

Threshold rule: No cells should contain less than 10 units (individuals, households or enterprises). You should provide the unweighted number of observations for each table, graph etc., even if in a separate file for us to check but not release. Remember, the threshold is 30 units for HMRC data.

Dominance rule: If we have a particularly dominant individual or business in the data being presented, then this could give away the presence of that unit in the data. Therefore the dominance rule states that the largest unit must account for no more than 43.75% of the total.

Degrees of freedom: Linear regressions must have a minimum of 10 d.o.f. (*in modeled output: d.o.f. = n - k*). Where the model is based solely on categorical explanatory variables, one of the coefficients should be suppressed for Statistical Disclosure Control reasons.

Residuals

Residuals that show individual data points should not be released. This includes plots, although a written description may be allowed.

Variable names

Variable names in datasets often seem to be little more than a random collection of letters and numbers when taken out of context so please ensure that the variable names in your tables are meaningful (i.e. it is unequivocal what they refer to without having to refer back to the documentation).

Secondary disclosure

Please check your output for secondary disclosure; e.g. where two 'safe' tables can be used in combination to reveal some potentially disclosive information. This can be a problem when presenting nested tables.

Sufficient explanation

Have you provided enough information for output checkers to be clear about what your output shows? You know your study area and the statistical techniques you have applied to the data inside-out, but it is unrealistic to expect output checkers to be experts on every area of inquiry and statistical technique. Please bear this in mind when submitting your output. It is a basic requirement that you supply some contextual information, and clear textual explanations of what each table and graph shows, and the underlying unweighted Ns. If you do not provide this we will contact you to request it, you will have to make changes and/or additions, and your output will *go back into the system*. All of this will delay the potential release of your output.

We understand that it is not unusual for journals to request additions or changes to a submitted paper and therefore you may request an output that is effectively an adjusted version of a previous one. However, you must treat this as an entirely new output and supply

all necessary information. **It is not sufficient to simply refer back to a previous output** – we need to be able to understand the new output fully (and be able to demonstrate that this output is safe in a 'standalone' sense).

Time management

We aim to be in touch about your output within 5 working days. The number of outputs can be very high at certain times of the year and at these times we may not be able to respond to you until close to the 5 working day deadline. The best case scenario is that we have found your output to be non-disclosive and release it to you within 5 working days. However, in a significant number of cases we might need to get back to you to clarify some details or there may be problems with the output that need to be addressed. This may mean that it takes more than 5 working days *overall* to receive your cleared output. Please bear this in mind and allow *more* than 5 working days. Moreover, you should keep in mind that you need to be able to access your SecureLab account after you have submitted your output to us in case we need to discuss details with you, or if you need to make any changes.

We deal with outputs in the order that we receive them as this is the fairest way; it is not our practice to 'leapfrog' outputs ahead of others so please don't ask (we know *your* output is important, but so are everybody else's).

Watchwords

Ensure that your outputs are **clear**, **unambiguous and within the scope of your research proposal**. You should only request material that you actually need.

14.5.   What if I want to present some initial findings to an informal departmental seminar?

In this case we are happy to assess your outputs, providing they are clearly presented and clearly explained. For example, a collection of tables could be produced in a Microsoft Word document, with an explanation after each table to describe the results.

As you will have learnt from the training course, **nothing should be written down from the screen** – it will not have been vetted for Statistical Disclosure Control. You must make an output request (see below) to release anything from SecureLab. The UK Data Service is responsible for ensuring that only non-disclosive results are released from the SecureLab.

With the above in mind, please do not refer to anything data-specific if you contact us (e.g. with a data query) – if you do it will mean that you have effectively removed something from SecureLab without it being SDC checked and **this constitutes a breach.**

!
WARNING

DO NOT
WRITE ANYTHING DOWN
FROM YOUR SECURE LAB WINDOW

THIS IS A SECURITY BREACH AND WILL RESULT IN SUSPENSION OF YOUR SECURELAB ACCOUNT

If you think that you will be able to explain your data query more clearly by referring to something data-specific then please make a note about it in a Word document in your project area and tell us where to find it. This approach means that nothing has been removed from SecureLab and no breach has been committed.

14.6.   Output checking of syntax files

You may wish to have some of your syntax released from SecureLab. This is not a problem but it must be content-checked before it can be released to you. We check for the following:

- no data tables or raw data copied in
- nothing left in that, in conjunction with information outside SecureLab, could identify and individual, household or business
- no descriptive sentences listed such as "there are 2 companies with x characteristics"
- no reference to the SecureLab server in the path directory of the data file location.

14.7.   How to request an output from your account

To request an output, please follow these steps:

1. Create a new folder in the SDC folder, named with your project number and date of request in the form of: 12345_YYYY_MM_DD
2. Save the files you would like us to release in the folder created in Step 1 (please give them a meaningful name, not something generic like 'output'.
3. Navigate to UK Data Service help pages to complete the online 'Output Request' form.

We aim to respond to your request within 5 working days.

14.8. Points to remember when submitting output requests

- Please allow 5 working days for a *first response* when submitting an Output request and to submit your requests in plenty of time before a deadline.
- Output requests are dealt with in the order in which we receive them and **you will not be able to submit a new output request until your original one is concluded** - any new output requests made prior to your original output request being concluded will not be processed.
- Please ensure that you are available to discuss, and/or amend, any problematic aspects of your output.
- Clearly label which tables or graphs include SecureLab data and which don't, if you are using a combination of SecureLab and non-SecureLab datasets.
- We cannot release **Excel (.xls/.xlsx) files** or **PowerPoint slides (.ppt/.pptx)** from the SecureLab.
- If there are any problems with your output that necessitate changes being made it is you that will make those changes. We do not make amendments to outputs for researchers.
- If you are submitting a LaTeX/TeX document please also include a PDF version in the same SDC folder, as this makes it much easier for us to check (thus meaning you should receive your output sooner).

14.9. Minimum requirements for ALL outputs

We have produced a checklist of **minimum requirements that an output must meet** in order for us to make a thorough statistical disclosure check and determine whether an output can be released. Minimum requirements are that:

- The output is one of the permitted output types.
- The results have clearly been written up, with information about the data source, sample and methodology included, as well as explanation of what each graph, figure etc. shows.
- Graphs, Figures etc. must be fixed images (e.g. JPEG).
- Unweighted cell counts must be provided for everything – e.g. graphs, figures, percentages, models results.
- Tables/figures must be correctly numbered and labelled.
- Variables must be given meaningful names, not just the labels from the dataset.
- The following embedded items must not be present in the output (you should use the 'Inspect Document' function to check this):
  - embedded documents
  - invisible content
  - hidden text.
- You must include the data citation in the output (**including the doi number**). This can be found in the Study Information files in your project area and for each dataset, by navigating to UK Data Service.

Your output must not deviate significantly from your original research proposal. We are obliged to check the content of each output against the research proposal you submitted and/or any change of scope that has been agreed with the data owner/s. Where these do not match up we will ask our Access Team to liaise with the data owner. You may need to set up a new project or make an addendum to the original proposal, depending on how significant the difference is between the proposal, or agreed change of scope, and the output submitted. The outcome will be decided by the data owner. To avoid this, please check back to your research proposal/agreed change of scope regularly to see if you are still within the previously agreed parameters. Contact us if you feel your project may have drifted and we will be happy assist you.

The following conditions should be met:

- Results should be neatly presented, in Word documents or TeX files. Excel spreadsheets, PowerPoint, Stata log files, and SPSS output files, for example, **are not acceptable for release**.

- Results should be clearly explained – it should be easy for output assessors undertaking the disclosure control to determine the meaning of the results in order to apply statistical disclosure control techniques.

If any of the minimum requirements are not met, your output will not be released. We will have to contact you for further information, thus delaying the release of your output and the outputs of other users.

14.10. Revising an output

If the output has been referred to you for revisions:

- Please save a revised version of the output file in the same SDC sub-folder that you created and append the new file name with '_updated_YYYY_MM_DD'. The original version and the new version should thus sit side-by-side in the same sub-folder.
- Once you have updated the document let the Support team know by replying to the same QTHELP email thread as the original output request.

14.11. Demonstrating impact

It is important to share how you think your research results may inform or benefit society.

Not only is this required by our funding council, the Economic and Social Research Council, but it also directly supports our shared purpose as a research community. Demonstrating that access to new data is valuable for research – and how that research may benefit society – helps us negotiate access to new sources of data and makes a strong case for continuing support.

On the online 'Output Request' form, you'll see a question about the impact of your research. Please give some considered thought when answering.

14.12. Case study solicitation

To help demonstrate the impact of your research, and the impact of the UK Data Service, we may get in touch with you to ask you to complete a case study questionnaire. This will ask you questions about your research, your main findings and the data you used. With your permission, a case study will be drawn up using your answers, and these will be added to our website. These will benefit other users and prospective data owners enormously.

14.13. A note on data citation

Data are a vital part of the scientific research process and proper data citation – including the doi number - should be a significant feature of research publications.

When submitting an output we ask you to include a full data citation in every output document. It is not necessary to include a citation under each table or figure within the same document.

The full citation can be found in the 'UKDA_Study_xxxx_Information' file in the 'Original Data' folder in your project area.

You can copy and paste the citation text if you use the Preview Pane to view files in a folder. Alternatively, you can open the data citation file from within the MS Word document by using the 'File – Open' command and locate the 'Study Information' file in the Browse window.

Below is an example citation for the 'Business Structure Database, 1997-2022: Secure Access' dataset:

Office for National Statistics. (2023). Business Structure Database, 1997-2022: Secure Access. [data collection]. 15th Edition. UK Data Service. SN: 6697, DOI: http://doi.org/10.5255/UKDA-SN-6697-15.

15. Finishing your project

15.1. What is the project expiry date?

When applying to access data for a project in the SecureLab, you will specify the start date and expiry date yourself. We will email you approximately **one month** before the expiry date is due, to remind you that the expiry date is approaching.

You should consider whether you have finished your project or whether you require more time to complete it.

15.2. If you have finished your project

We encourage you to maintain syntax that will allow you to recreate data and analysis. Remember that we are unable to keep users' derived data files in the long-term. However, we will keep syntax – **but only those files saved in your Syntax folder**. You may also request your syntax files to be released as an output, as long as they do not include data or pathways to the SecureLab server.

The outputs that we release to you will also be saved, although not in the SecureLab area itself. Other files in other folders will be removed when your project expires.

How long do we keep a finished project in our system in order for you to re-visit it at a later date? Indefinitely!

Please ensure that you have requested all necessary files to be released to you (subject to SDC checks) before project closure.

16. General do's and don'ts

There are a lot of things to remember about using the SecureLab. As a reminder, here are some guidelines that we please ask you to remember:

16.1. Do remember

- That your session is recorded by 'SmartAuditor' for security and training purposes.
- That the screensaver is activated after five minutes of inactivity.
- That you will be asked to change your password every twelve months.
- To familiarise yourself with the ['Code of practice'](#).
- That if you have a data query and feel that it would be best explained by referring to some specific aspect of the data, you should make a note in Word and save this in your project area. Then, you can email the support team to tell them where to find this note. **Do not write anything down from the screen and email it to us** – this constitutes a serious breach (see below).
- If you experience any issues while using SecureLab please **do not** email us error messages etc. Instead, carefully record the details in a clearly labelled Word file and use the ['website/technical issues' online form](#) to tell us to inform us where we can find that file. In this way, nothing is removed from SecureLab, and no breach has occurred.
- You can only use results that have been SDC checked and released by us to you. No information regarding SecureLab data, including general trends, should be reported or discussed in any way outside of SecureLab without first undergoing SDC and release. This includes any details that you may have kept in your head from the session when you did analysis in the SecureLab.
- To **contact us if you are not sure about anything** related to secure data and related policies.

16.2. Do not

- **Write anything from the screen – this is a breach and a disciplinary offence.** We have installed Microsoft Office so that you can make notes and save them in your SecureLab account. It is hard to be 100% sure that something you write down doesn't constitute data of some kind so the best option is to copy nothing down from the screen.
- Take screenshots from your working session.
- Try to log into the SecureLab from outside your agreed access environment (most commonly your institution).

- **Share your password with anyone** – not even a member of the UKDS Support team or other researchers working on the same project.
- Discuss individual observations or data in emails to the Support Team as this means you are effectively removing data from the SecureLab environment. If you need to refer to a specific case, please add a note in your project folder and let us know where to find it.
- Allow unauthorised people to see the data/un-cleared outputs over your shoulder.

Finally... DO please tell us if there is any way we can improve our service to better suit your needs.

17. Help and support

Contacting the UK Data Service for help

For advice on common technical problems and support on technical issues please see section 18 *'Advice and technical support'*.

Support for researchers accessing data via the SecureLab (formerly the Secure Data Service), is provided by the UK Data Service.

To contact us for help and support, please use the relevant online form by navigating to UK Data Service help pages.

If you have a query about the data you are accessing, use the **Analysis/using data** form.

If you would like us to release a statistical output to you, use the **Output release** form (note you no longer need to complete an Output Request form within your account).

If you experience a technical difficulty (for example, you cannot log into your account), use the **Website/technical issues** form.

(IMPORTANT: when using this form, make sure you identify the correct issue by clicking on the 'Type of website/technical issue' drop down menu, and choosing an option relating to Secure Access).

If you wish to upload data to your account, please use the 'SecureLab import data request' form.

If you wish to import syntax to your account, please email support@ukdataservice.ac.uk.

For queries about making an application to access data in the SecureLab, please email secure.applications@ukdataservice.ac.uk.

18. Advice and technical support

18.1. Technical problems

Unfortunately, sometimes IT doesn't work. This is especially the case of network dependent systems such as the SecureLab. However, you might find the following points useful. Always try restarting your machine – this often resolves problems. Also, remember that the SecureLab cannot be accessed during the weekly maintenance period on Tuesday mornings until around 12.30. Before you contact us, note the following details (which will help us to identify and solve the problem):

- What date and time did the error occur (please be as accurate as possible)?
- Have you rebooted your PC – is the error reproducible (and please note the time you tried this)?
- Please describe the error and what you were doing when it occurred
- Please provide precise details of any error messages that occur (verbatim). In order to avoid committing a breach you should paste/type the error message into a Word document and then use the 'website/technical issues' online form to tell us whereabouts in your project area we can find it. In this way, nothing is removed from SecureLab, and no breach has occurred.

18.2. Some common errors, and possible solutions, are listed below:

I try to click on the log in page but I can't get through to the username and password page.

Have we got your correct IP address? Usually this error occurs because you are trying to access the SecureLab from a computer that our secure server firewall doesn't recognise. Did you recently change your computer? Check with your IT support to confirm your computer's IP address, and check that it is a 'static routable' IP address (dedicated to your computer and doesn't change every time you start the machine).

Call us with your confirmed IP address and we'll update our firewall if necessary.

*When I click on the SDS Desktop icon, the SecureLab window doesn't launch. Nothing happens.*

This could be a software error at your end. Uninstall your Citrix client software, and install the latest version (visit receiver.citrix.com). Restart your computer and try again. Your IT support may have to do this for you.

The Citrix software is the small software application that you installed on your computer just before we provided you with your username and password.

I was logged in; now the screen is locked and I can't get back in.

This could have been caused by a network connection issue, either at your institution's end or ours – it is difficult for us to tell.

Users can now restart their own sessions by clicking on the downwards arrows > restart.
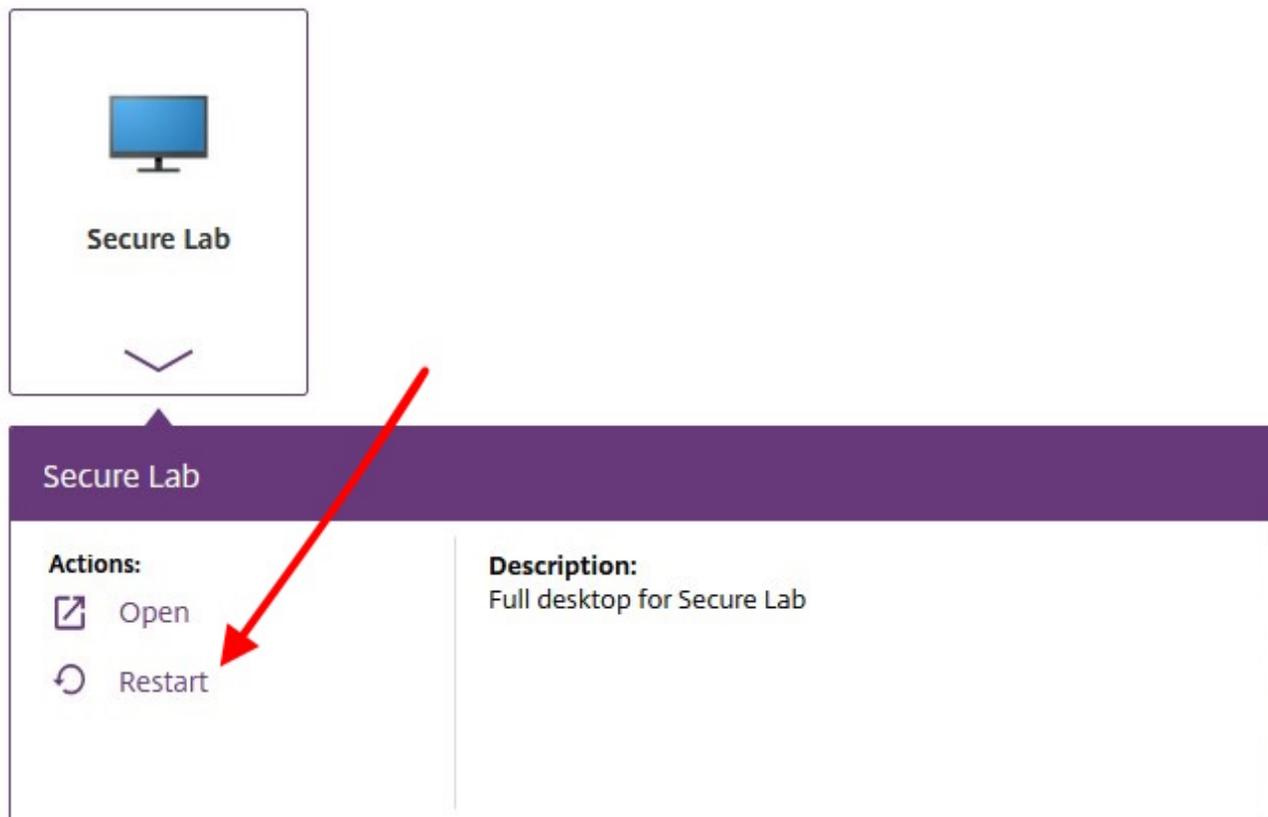
In this case, please use the online form (see below) and we will log you off, allowing you to log back in again.

When you have tried the above…

…and find that the problem is not resolved, please contact us using the ['Website/technical issues' online form](). Please remember to paste/type any error message (verbatim) into a Word document in your project area, and use the form to tell us where this document is. This methods ensures that you do not inadvertently commit a breach (e.g. by emailing this information to us) as nothing has left SecureLab.

19. General problems and FAQs

If you experience any difficulties using the SecureLab, help is at hand.

19.1. FAQs

First, check the ['Frequently Asked Questions']() for the SecureLab by navigating to the UK Data Service website.

We keep this updated as we receive similar questions from different researchers. There is a good chance that your question will be answered here.

19.2. Personal contact

If your question is not answered on the website by use of the FAQs or the appropriate on-line forms then, please get in touch with us directly by email and telephone:

Support is normally available 9.00 to 17.00, Monday to Friday (excluding public holidays).

T 01206 874968 (9.00 to 12.00)

E support@ukdataservice.ac.uk

19.3. Support available

We are happy to provide information and guidance, including:

- advice on projects (for example, finding suitable data)
- how to apply to use data through the SecureLab
- how to use the SecureLab (for example, where files are stored)
- how to request outputs and Statistical Disclosure Control
- extending your project and using more data sources.

In addition, we can negotiate with data owners for access to data, particularly as we meet strict international standards in data management and security. If you think that we might be able to help you to access data that are not currently available from the SecureLab then please get in touch.

19.4. Your service

Please remember that this is your service – and our shared responsibility as a research community.

19.5. Feedback

If you have any ideas about how we can improve the SecureLab, we would be pleased to hear from you. Please contact us at any time.

20. UK Data Service activities

We do more than provide secure access to confidential data. We also support researchers in other ways. Here are some of the ways we help to promote applied research.

20.1. Organise workshops

This is a chance for anybody with a stake in the SecureLab (users, staff, funders or data suppliers) to come together to share knowledge about general strands of research (such as labour markets), or particular data sources (such as the *British Household Panel Study*).

20.2. Negotiate for access to more data

The high security standards we meet put us in a strong position to negotiate for access to new data sources from a range of suppliers to enable our users to conduct more effective research.

20.3. Publicise research

We provide details of research undertaken on our website and regular e-bulletins. Everybody in our community can see the research that the UK Data Service is helping to support – which is especially useful for users and good news for data owners in particular.

20.4. Data dissemination standards

The SecureLab is one of a number of core services provided by the UK Data Service. We are at the forefront of developing technologies and improving standards to disseminate data, documentation and metadata. This benefits researchers because we can supply a better service to you.

www.ukdataservice.ac.uk

help@ukdataservice.ac.uk

+44 (0) 1206 872143