Secure Access User Agreement

13 November 2023

Public

Version: 11.00

Table of contents

1. Scope

UK Data Service SecureLab Registered Users must agree to this Secure Access User Agreement ("Agreement") and any other document referred to herein before being issued credentials to access Controlled Data from the SecureLab.

2. Introduction

This document represents one of the steps that prospective Registered Users of the UK Data Service SecureLab must fulfil prior to being able to access data from the SecureLab. The Agreement must be signed by the Registered User and their organisation, and returned before the Registered User can receive a username and password for remote access to the SecureLab. The Agreement demonstrates that the prospective user and their organisation understand the seriousness of the undertaking, and that they each understand the penalties that may be imposed for non-compliances with security or confidentiality.

3. The Parties

This Agreement is agreed between:

1. The individual Registered User of UK Data Service SecureLab.
2. The organisation responsible for the Registered User.
3. The University of Essex acting by its UK Data Archive of Wivenhoe Park, Colchester, CO4 3SQ (the "Data Service Provider").

In the event of the University of Essex ceasing to be a legal entity, this licence will be transferred to the Economic and Social Research Council (ESRC) or its successors.

IT IS HEREBY AGREED:

4. Definitions of terms

Data Collection: The dataset(s), documentation, metadata, occasionally code, provided by the Depositor for dissemination to the Designed User Community and curated by the UK Data Service in accordance to the Collections Development Policy and Selection and Appraisal Criteria.

Designated User Community: The UK Data Service's Designated User Community is made up of social science and related data users within Higher and Further Education in the UK, however services are designed for all users. All users are expected to have a basic understanding of social science methods and techniques relevant to the data collections being accessed.

Registered User: A user who has registered with the UK Data Service and therefore agreed

online to the End User Licence Agreement.

ESRC Accredited Researcher: A Registered User to whom the UK Data Service and the data owner(s) have granted access to Controlled Data for the purposes of statistical research.

DEA Accredited Researcher: A user accredited under the Digital Economy Act 2017 (DEA) to access data for research purposes under the DEA and the Statistics and Registration Services Act 2007.

Data Service Provider: The person(s) or organisation(s) that directly provide the User with the Data Collections (on behalf of the Service Funder) and identified in the Metadata applicable to that Data Collection. A Data Service Provider may also provide user support, training, and research data management advice.

UK Data Service SecureLab: A service established at the University of Essex funded by the Economic and Social Research Council intended to promote excellence in research by enabling safe and secure remote access for researchers to Controlled Data via the Five Safes Framework.

Controlled Data: UK Data Service Data Collections made available to ESRC Accredited Researcher(s) and DEA Accredited Researcher(s) via the Five Safes Framework. Also referred to as Secure Access data.

Data Protection Legislation: Laws relating to data protection, the processing and use of personal data, including the Data Protection Act 2018 (DPA 2018), General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR), the UK General Data Protection Regulation 2018 (UK GDPR), and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and any successor legislation to the GDPR.

Applicable Law: The Digital Economy Act 2017 (DEA 2017), the Statistics and Registration Services Act 2007 (SRSA 2007), and any laws, regulations and secondary legislation, as amended or updated from time to time.

Secure Researcher Training: Mandatory training provided to ESRC and DEA Accredited Researchers before they can access Controlled Data.

Personal Data: Are defined as in accordance with the UK General Data Protection Regulation (UK GDPR) Article 4(1) and the Data Protection Act (DPA) 2018 s3(2) as: data that relate to an identified or identifiable natural person, be it directly or indirectly, taking into account other information derived from published sources.

Personal Information: Information that relates to and identifies an individual (including a body corporate) taking into account other information derived from published sources (as defined in section 39(2) of the Statistics and Registration Service Act 2007).

Data Controller: The natural or legal person, public authority, agency or any other body which

alone, or jointly with others, determines the purposes and means for the processing of Personal Data.

Data Owner: The natural or legal person, public authority, agency or any other body which alone, or jointly with others, holds the copyright and associated intellectual property rights in a Data Collection.

Depositor: The person named on the Deposit Licence Agreement having sufficient responsibility to grant particular rights on behalf of a Data Collection. The depositor may be the principal investigator, creator or the copyright owner of a Data Collection, or authorised to grant the Deposit Licence Agreement.

5. Agreement

General Terms and Conditions

1. All Registered Users must satisfactorily complete the mandatory Safe Researcher Training which allows the Data Service Provider to ensure that Registered Users are fully aware of any penalties which they might incur if they do not comply with this Agreement or compromise the security and confidentiality of the data. Registered Users may be required, if appropriate, to reattend the training according to UK Data Service requirements. Information about training received may be shared with other relevant services such as the Office for National Statistics Secure Research Service (ONS SRS).
2. Access to the Personal Information and/or Personal Data is being provided for the statistical and research Purpose outlined in the Accredited Researcher application form. Personal Information and/or Personal Data shall not be used for any other purposes without the prior written consent of the Data Service Provider and where necessary the Data Owner(s)/Data Controller(s).
3. The Registered User shall not disclose nor compromise any of the Personal Information or Personal Data from the individual records obtained or produced from the Data Collection(s) pursuant to this Agreement to (i) anyone other than those approved for the same research Purpose and (ii) UK Data Service staff involved in the review of the outputs for the statistical disclosure control.
4. The Registered User shall ensure that no attempts are made to link the Personal Information or Personal Data to any other files in order to relate the particulars to any identifiable individual person, business or organisation unless such data linkage exercise has been explicitly approved at the time of the project application, or approved subsequently as part of a special request to the Data Owner(s)/Data Controller(s), or their delegated decision-making body.

5. On termination of the Agreement for whatever reason, all access to the Personal Information or Personal Data related to the Purpose shall cease forthwith, and access will be denied.
6. The Data Service Provider reserves the right to monitor, record, and audit, or to request a written report from the Registered User regarding the use, and activities relating to the use, of the Personal Information and/or Personal Data by the Registered User during the lifetime of this Agreement. This includes the right of entry to the premises where the data are accessed.
7. The Registered User is responsible for liaising with their organisation to ensure that all technical requirements for accessing SecureLab as detailed in the “Technical Requirements” section are met. This includes seeking necessary approvals, assistance, or resources from the organisation to comply with the stipulated conditions. The Registered User must ensure that their organisation is informed about, and supportive of, the technical specifications and security measures required for SecureLab access.
8. It is the responsibility of the Registered User to provide all necessary information about the device used to connect to the SecureLab for the checks and verifications carried out by the Data Service Provider. Timely and accurate provision of this information is essential for the activation and maintenance of the SecureLab account.
9. The Registered User must observe good security measures when accessing the SecureLab, including but not limited to, locking the screens when leaving the device unattended, ensuring credentials are not shared, saved or cached in the web browser, using privacy filters if there is a risk of overlooking the device.
10. Any incidents of unauthorised access to, processing of, or disclosing of, the Personal Information and/or Personal Data must be reported immediately to the Data Service Provider.
11. The Agreement is subject to review and without limitation whenever a change in the law, contracts for services with third parties, other procedures or other relevant circumstances takes place.
12. Any non-compliance with this Agreement will result in the immediate imposition of penalties as outlined in the UK Data Service Licence Compliance Policy.

Technical Requirements

1. 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.

2. 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.

3. 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 organization.

4. 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.

5. The Registered User must ensure that no screen capture tools are running on the device during SecureLab access.

Output Release

1. The Registered User shall not reproduce to any extent from the UK Data Service SecureLab virtual environment any original dataset or copies or subsets of any Personal Information and/or Personal Data.
2. Any outputs to be removed from the UK Data Service SecureLab by the Registered User must first be screened by the UK Data Service to ensure that there is no risk of disclosure of Personal Information or Personal Data, or information that may lead to the identification of an individual person, business or organisation. Outputs may also be screened by other services such as the ONS SRS and/or Data Owner(s). Only outputs that have been screened and cleared by the UK Data Service will be sent to researchers. Any output sent to the researcher by the UK Data Service will be considered non-confidential.
3. The Registered User is responsible for applying the rules and regulations for disclosure risk analysis as specified by UK Data Service statistical disclosure guidelines (provided during training) prior to submission of analytical outputs for clearance and release.
4. The Registered User agrees to work with the Data Service Provider to meet the requirements of safe outputs. In the event that the Data Service Provider decides not to release the proposed output, the Registered User will have an opportunity to attempt to demonstrate to the Data Service Provider and, where appropriate, the Data Owner(s) that the output is safe. However, the final decision to release an output rests with the Data Service Provider, not the Registered User.

5. The Data Service Provider reserves the right to release in whole or in part, an amended version or not to release at all, as the Data Service Provider deems appropriate, any proposed output.
6. The Registered User must provide a description of variables used, new variables/measures/indices created, documentation of datasets and programs used in producing analytical output(s) to ensure the Data Service Provider's staff have the information they need to make a judgement on the output(s) requested for release.
7. The Registered User will inform the Data Service Provider of any publication that contains outputs released by the UK Data Service.

Acknowledgements and Copyright

1. The Personal Information and/or Personal Data and related documentation shall at all times be and remain the sole and exclusive property of the Data Owner(s). This Agreement pertains to the use of the Personal Information and/or Personal Data and related documentation to produce a "proposed output" for research purposes and that nothing contained herein shall be deemed to convey any title or ownership interest in the Personal Information and/or Personal Data or the related documentation to the Registered User.
2. The Registered User acknowledges that the Personal Data is handled at all times in accordance with the Registered User's obligations under the Data Protection Act 2018 and UK GDPR.
3. Copyright of outputs may be held singly or jointly by the Registered User(s) who created them, their institution(s) or their funder(s) according to the Registered User's funding and institutional agreements.
4. The Registered User must cite, in any publication, whether printed, electronic or broadcast, that contains outputs released by the UK Data Service, the Data Collection(s) used, in the form specified in the documentation and metadata accompanying the dataset or notified to the Registered User.

6. Declaration

The Declaration is to be agreed and signed by the applicant, who will be the Registered User requiring access to the Personal Information and/or Personal Data for his/her own research needs, and by an appropriate officer (in the Research & Contracts Office, or equivalent) from the organisation from which they will be accessing the UK Data Service SecureLab.

Where there is a research team, each member of the team will need to be a DEA Accredited Researcher/ ESRC Accredited Researcher whose research Purpose has been approved.

By signing this Declaration, I, the Registered User, confirm that:

- All the information I provide in support of an application to access Controlled Data via the UK Data Service SecureLab is true and accurate.
- I have read, understood and agreed to the End User Licence Agreement.
- I have read, understood and agreed to the UK Data Service Licence Compliance Policy.
- I have read and understand the conditions specified in this Agreement.
- I will abide by any other requirements communicated to me by the Data Service Provider relating to the use of Personal Data and/or Personal Information.
- I will comply with all of the policies and operating procedures presented to me in the training session.

I declare that the Personal Information and/or Personal Data provided to me shall be kept secure and confidential according to the terms of this Agreement.

I understand that:

- The Data Service Provider may hold and process information submitted by me in my Accredited Researcher application for validation and statistical purposes, and for the purposes of the management of the service and may also pass such information to other parties such as Data Owner(s), Data Controller(s), Data Depositor or their nominees.
- If I use the Data Service Provider Safe Room to access SecureLab, my image will be recorded on CCTV and will be held and processed by the Data Service Provider for the purposes of security and management of the service.
- If I use the SafePod Network[1] to access SecureLab, the University of St Andrews will hold and process information submitted by me and will pass this information to the Data Service Provider for the purposes of managing my bookings.
- If I use the SafePod Network to access SecureLab and CCTV is required as a condition of my booking, then the University of St Andrews will hold and process my recorded images for the purposes of management of SecureLab security via the SafePod Network service.
- The Data Service Provider reserves the right to scrutinise any analytical outputs,

[1] https://safepodnetwork.ac.uk/

products or publications for disclosure control purposes before publication.

- If I knowingly or recklessly disregard the terms of the Agreement this will be an offence under sections 170 and 171 of the DPA 2018 that may incur financial penalties. It may also be an offence under the Statistics and Registration Service Act 2007 and Digital Economy Act 2017, if I disclose Personal Information without the written authority of the National Statistician or other Member of the UK Statistics Authority.
- My lawful use of Personal Information and Personal Data is only for the Purpose(s) of statistical research that will serve the public good.
- Any information accessed through the UK Data Service SecureLab will only be used for the Purpose(s) stated in the project application.
- I am required to bring directly to the attention of the Data Service Provider any matters or events that may affect my obligations under this declaration.
- I am authorised to access Personal Information and Personal Data only when I receive from the Data Service Provider a written confirmation, and only until the end date in that written confirmation.

Registered User's signature	
Registered User's full name and title	
Organisational address	
Date	

I, as an authorised organisational signatory, confirm that the Registered User is attached to my organisation and understand that said organisation could be liable to the penalties outlined in the UK Data Service Licence Compliance Policy in the event of a breach of this Agreement by the Registered User.

Organisational signature	
Name of organisational signatory	
Position of organisational signatory **(must be an authorised signatory of the organisation)**	
Date	

www.ukdataservice.ac.uk

collections@ukdataservice.ac.uk

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