UNIVERSITY OF PLYMOUTH

Security and Usage Policy for the ONS Secure Room and Remote Access (SUP_ONS_UoP)

Author: Cassandra Paxton-Denny (TIS), Alex Gibson (CfCC), Emma Wainman (Legal and Compliance), John Martin (R&I)

Date: 26/04/2024

Document Security Level: **INTERNAL ONLY**

Document Version: 0.1

Related Policies: GDPR and working from home
End user device allocation policy

Version history and sign-off

Version	Author(s)	Position(s)	Revision / Approval Details	Date/Time
0.1	CPD	IT BP	Initial draft created	26/04/2024
0.2	CPD	IT BP	Technical compliance	26/04/2024
0.3	AG	ONS Coordinator	Non-technical compliance	14/05/2024
0.4	EW	FoI and DP Specialist	Legal and Compliance Review	31/05/2024
1.0	**ISG**		**Approval**	
			Review date (3 years from ONS approval of attestation)	

*Please indicate document approvals in **bold**.*

Introduction

1.1 Purpose

This policy is intended to protect you as a researcher as well as the University of Plymouth, and to ensure that you and the University are not in breach of the security and data requirements to handle research data accessed via the ONS SRS or IDS services.

1.2 Scope

The rules in the Security and Usage Policy for the ONS Secure Room and remote Access at the University of Plymouth are mandatory for all ONS Accredited Researchers (AR) who have been approved remote access to ONS level 3 data.

1.3 Definitions

- Accredited Researcher (AR) – an individual who has met the ONS's Accredited Researcher criteria (source: DEA Code of Practice 2017), undertaken the Safe Researcher Training (SRT) or the Safe Users of Research Environment (SURE) training, successfully completed the assessment and had their projects approved by the Microdata Release Panel (MRP) or Research Accreditation Panel (RAP).
- Accredited Projects - Research proposals approved by the ONS Accredited (MRP) or Research Accreditation Panel (RAP), on behalf of the National Statistician.
- ONS Coordinator – single point of contact for all matters relating to SRS/IDS operational access for the University.
- Data Protection Legislation - UK GDPR and Data Protection Act 2018.
- Privacy screen – a physical filter or panel that can be attached to your computer monitor, laptop or other electronic display to protect your privacy by limiting the viewing angle of your screen making it difficult for people sitting beside or behind you to see what is on your screen. These can be purchased from Proband on UNIT4.
- Remote access - Secure VPN connection using the VPN software provided by University IT services.
- Secure Room – Accredited Researcher Secure Room to access ONS data located Rm 338, Cookworthy Building (specific to access by room owner).
- Severe Breach – any breach of this Policy or related University Policies that might endanger the present and future fruition of access to the ONS SRS services by UoP staff.
- University Systems – any hardware, software, data, network access, third party services or online services provided or arranged by the University of Plymouth.

Policy Terms

2.1 Registration to the SRS/IDS Services at UoP

2.1.1 In order to request access the ONS SRS or IDS services, each prospective User must submit an ethics application via PEOS, attach the required evidence and provide their AR credentials, including

- AR ID number
- ID number of their SRS/IDS project(s)
- device ID (this can be found on the base of your PC or on the lid of your laptop)
- connection location (Secure room or remote access)
- provisional connection dates.

2.2 Access to the SRS Secure Room on University premises

2.2.1 Access to the SRS and/or IDS environment on campus is only allowed from an ONS approved Secure Room and not from any other organisation premises, including common areas such as a staff restaurant or coffee lounge.

2.2.2 ARs are only permitted to connect to the SRS/IDS environment using their University-managed device, which must be managed under an organisational ICT policy or equivalent. The use of a personal or off-image devices is not permitted.

2.2.3 The use of mobile phones and other electronic devices (other than your University-managed device) is not permitted whilst accessing the SRS/IDS environment except to allow for Multi-Factor Authentication procedures at the start of the session.

2.2.4 Your device should be placed in a way to minimise shoulder surfing. The back of the screen should face the door so it cannot be overlooked, if this is not possible then side on with a privacy screen would suffice.

2.2.5 Data accessed via the SRS/IDS environment must be kept confidential and handled in accordance with Data Protection Legislation. It is a criminal offence under the Statistics and Registration Act 2007 to unlawfully disclose personal information held by the ONS.

2.2.6 ARs must only access the data for the purpose of working on defined and Accredited Projects.

2.3 Access to the SRS via VPN Remote Access

2.3.1 Remote access to the ONS SRS/IDS environment must be via the dedicated ONS VPN Remote Access client to prevent and/or minimize the risks for the confidentiality of the data accessed.

2.3.2 Remote access to the ONS SRS/IDS environment must not be from any public space such as an Internet Café or restaurant/cafe.

2.3.3 ARs are only permitted to connect to the SRS/IDS environment using their University-managed encrypted device, which must be managed under an organisational ICT policy or equivalent. The use of a personal or off-image devices is not permitted. Some ARs are not eligible for a University-managed device under the device allocation policy and will need to request an exemption as part of the process.

2.3.4 The use of mobile phones and other electronic devices (other than your University-managed device) is not permitted whilst accessing the SRS/IDS environment except to allow for Multi-Factor Authentication procedures at the start of the session.

2.3.5 Access from home must be from a separate room to other members of your household. If this is not possible, your device should be placed in a way to minimise shoulder surfing and if this is not possible then side on with a privacy screen is permissible.

2.3.6 You must you lock your screen when leaving the room.

2.3.7 You must ensure your home Wi-Fi network has been secured by ensuring it is up to date and the default administrator username has been changed and the password has been reset to a strong administrative password.

2.3.8 ONS specify users must have a minimum Internet connection speed of 2.8Mbps

2.3.9 Data accessed via the SRS/IDS environment must be kept confidential and handled in accordance with Data Protection Legislation. It is a criminal offence under the Statistics and Registration Act 2007 to unlawfully disclose personal information held by the ONS.

2.3.10 ARs must only access the data for the purpose of working on defined and Accredited Projects.

Governance

3.1 Reporting Incidents

3.1.1 The User must notify the University's ONS Coordinator via email of any suspected security breach and/or an SRS/IDS data leakage within 24 hours from the incident.

3.2 Policy enforcement and breach sanctioning

3.2.1 ONS have the right to implement sanctions which can include immediate suspension of any remote access or disconnecting a device for a failure to abide by this policy.

3.2.2 Users violating the above conduct rules will be liable to disciplinary actions by the University including instant temporary ban from accessing the ONS SRS/IDS environment, with the possibility for the ban to become permanent.

3.2.3 Breaches of conduct must be reported in a timely manner to the University's ONS Coordinator, who will administer proportionate sanctions to the User(s) in the first instance and/or report the violation(s) to the HoS in case of particular gravity.

3.3 Review and Change Requests

The policy will be reviewed annually or as necessary.

User declaration form

This form must be signed by the User and submitted via the ethics application process in PEOS.

Hereby I certify that I have read and understood the terms of the Security and Usage Policy for ONS Secure Room and Remote Access at the University of Plymouth.

PRINT name:

SIGNED by:

Adherence to the content of this document and the documents cited, is obtained on DATE / / .

You will be personally liable if you contravene this consent.