SGUL Basic Identity Verification SOP

Document Information	
Document Name	SGUL Basic Identity Verification SOP
Owner	Research Data Management Service
Issue Date	31/01/2020
Approved By	Chair of SGUL IGSG
Next review	31/01/2022

Document History		
Version	**Date**	**Summary of change**
0.1	06/09/2017	First draft for discussion
0.2	21/09/2017	Amended with comments from Adam Witney and Michelle Harricharan
0.3	26/02/2018	Amended with comments from IGSG
1.1	31/01/2020	Document owner changed

1 Scope

SGUL requires suitable assurances that the applicants requiring access to de-identified, controlled access research data held at St Georges, University of London (SGUL) are genuine. The objective is to undertake sufficiently robust verification processes to confirm that the applicant is the owner of the claimed identity and that the identity is genuine.

2 Responsibilities

2.1 The Information Asset Administrator (usually the Principal Investigator (PI) or the Information Asset Owner (usually the Head of Institute if the PI is no longer at SGUL), has the responsibility for ensuring that applications for data under their stewardship are subjected to suitably robust investigation. The Information Asset Administrator will provide the necessary evidence confirming the identity of the applicant acquired through the procedures in this SOP. He/she will also provide the necessary assurances to the SGUL Senior Information Risk Owner (SIRO) for the release of the requested information asset. The Information Asset Administrator is the risk owner of the relationship with the external party who has requested the information asset. If the application is approved, the Information Asset Administrator is responsible for ensuring that a data sharing agreement between SGUL and the receiving organization is agreed and signed. The Information Asset Administrator is also responsible for ensuring the secure transmission of the information asset to the applicant once the data sharing agreement has been signed.

2.2 If the Information Asset Administrator, after robust investigation, cannot provide the necessary assurances or evidence that the applicant is the owner of the claimed identity and that the identity is genuine, then the responsibility for verifying the identity of the applicant falls to the SGUL SIRO.

2.3 The Senior Information Risk Owner's (SIRO) decision on the release of the information asset will be final, with the exception of a formal protest by the Information Asset Administrator. In such circumstances the Information Asset Administrator must inform the SIRO of their appeal to the SGUL Chief Operating Officer, who will make the final decision.

3 Procedure

3.1 The primary contact for all applications for access to de-identified, controlled access research data held at SGUL is the St George's Research Data Management (RDM) Service. The SGUL Research Data Support Manager will send requestors the official Data Access Application form to complete. Students will not be able to apply for access to data, but supervisors may be able to

apply on their students' behalf. No guarantee can be offered for access to data for student projects.

3.2 The Data Access Application form is checked for completeness by the Research Data Management (RDM) Service, ensuring that the Applicant has provided the information outlined below:

Name; Job Title; Name of organisation receiving the information asset; Business address including research department; telephone number; email address and business website; contact information for the organisation's SIRO (or another accountable officer such as the Data Protection Officer, or a representative of the Legal team or Information Governance Office). An organisation without these offices, or an equivalent of these offices, will not be considered for access to St George's data as we will not have the assurances that the organisation is prepared to handle more sensitive datasets.

3.3 The Research Data Service will forward the completed Data Access Application form to the Information Asset Administrator who will use their professional networks to ensure that the applicant is the owner of the claimed identity and that the identity is genuine.

3.4 The Information Asset Administrator must collect written evidence from officials at the receiving institution that the identity is genuine and that the owner of the identity has, indeed, made a request for the identified dataset from St George's, University of London.

3.5 Once the Information Asset Administrator has compiled evidence that the identity is genuine and that the applicant is indeed the owner of the claimed identity, he/she must complete the Data Access Application Form with his/her recommendation for the release of the dataset and forward the form, along with the evidence collected, to the SIRO for a final decision.

3.6 If the Information Asset Administrator cannot find strong evidence that the applicant is indeed the owner of the claimed identity and that the identity is genuine, the information Asset Administrator can complete the Data Access Application form requesting the SGUL SIRO verify the identity of the applicant.

3.7 The SGUL SIRO, on receipt of the application, will make a decision on the release of the information asset based on the information provided in the application.

3.8 If the application is approved, the Information Asset Administrator, as the risk owner of the relationship with the external party, will make arrangements for the signing of an appropriate data sharing agreement under advice from the St George's Data Protection Officer and legal team before the data can be transferred.

3.9 If the application is not approved, then the Information Asset Administrator and the SGUL RDM Service are advised of the outcome by the SIRO. The SGUL RDM Service will work with the Freedom of Information Officer to deliver the rejection.

3.10 The Information Asset Administrator may appeal the decision of the application. In such circumstances the Information Asset Administrator must inform the SIRO and the SGUL RDM Service of their appeal to the SGUL Chief Operating Officer, who will make the final decision.

Document Control and Approval

The Senior Information Risk Owner is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the IG Toolkit and SGUL Policies.

This document is **COMMERCIALLY CONFIDENTIAL** and is therefore restricted in use and is not available to members of staff on the SGUL Intranet.

This procedure was approved by the Senior Information Risk Owner on 27/02/2018 and is issued on a version controlled basis under his/her signature.

Signature: Date: