SOP Title Reference: **Data Protection**	Last Reviewed: **09/10/2023**	Last Revised: **23/06/2021**	
Author: **Information Services**			

St George's University of London Policies and Procedures

Data Protection Policy

(see also related documents 'Guidance on Data Protection')

Contents

1. Introduction

The Institution needs to keep certain personal data, for example about its staff and students, to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Institution must comply with the Principles which are set out in UK Data Protection Legislation.

2. Principles

Personal data shall:

- be processed lawfully, fairly and in a transparent manner
- be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- be adequate, relevant and limited to what is necessary in relation to the purposes
- be accurate and, where necessary, kept up to date
- be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes
- be processed in a manner that ensures appropriate protection against unauthorised or unlawful processing, accidental loss, destruction or damage

The Institution and all its staff who process personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Institution has developed this Data Protection Policy.

Data Protection Legislation places an additional responsibility on the University to demonstrate our compliance with these Principles, which we do through the institution’s Register Of Processing Activities (ROPA).

3. Status of the Policy

This policy has been approved by Council and any breach will be taken seriously and may result in more formal action.

Any member of staff or student who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Institution's Data Protection Officer in the first instance.

4. Notification of Data Held and Processed

All staff, students and other users are entitled to:

- Ask what information the Institution holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed about what the Institution is doing to comply with its obligations under Data Protection Legislation

5. Responsibilities of Staff and Students

All staff and students are responsible for:

- Checking that any personal data that they provide to the Institution about themselves is accurate and up to date
- Informing the Institution of any changes to information about themselves which they have provided, e.g. changes of address
- Checking any information that the Institution may send out from time to time, which give details of information that is being kept and processed

If, as part of their responsibilities, staff process information about other people (e.g. students, members of staff, participants in research studies), they must comply with this Policy, and with the University's Guidance on Data Protection and its guidance on other relevant aspects of data protection.

Students who use the Institution's computer facilities may, from time to time, process personal data. If they handle personal data they must do so in line with the University's policies and, where relevant, seek advice or guidance from the Institution's Data Protection Officer.

6. Data Security

The need to ensure that all University data, especially personal data, is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

- All University data which they handle is kept securely
- All personal data which they handle is kept securely
- Personal and sensitive personal data is encrypted and is sent using appropriate secure mechanisms, especially when being sent outside the Institution
- Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party

University members are also responsible for ensuring that data is disposed of securely using appropriate methods. Personal data held on paper must be disposed of as ‘confidential waste’ via an approved service. Advice on the disposal of electronically stored data should be obtained by contacting IT Services.

More detailed guidance on data security, and staff responsibilities for data security, is contained in the Guidance on Data Protection document.

7. Rights to Access Information

Staff and students and other users of the Institution have the right to access any personal data that is being kept about them. Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer.

The Institution aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month of receipt of a request, subject to confirmation of ‘proof of ID, and unless exceptional circumstances prevent this from being possible. In such cases the individual will be contacted direct to discuss the situation further.

The right of access is just one of the individual’s rights under Data Protection law. The full list of rights comprises:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

For advice on how to exercise any of these rights please contact the Data Protection Officer.

8. Publication of Institution Information

Certain information about members of the Institution will be ‘in the public domain’. This would include, for example, information on staff contained within externally circulated publications or externally accessible webpages. Any individual who has good reason for wishing certain details about themselves to remain confidential outside the Institution should contact the Data Protection Officer.

9. Lawful Basis

The need to process data for normal business purposes forms part of the contract between SGUL and its staff and students. Details of this processing has been communicated to all staff and students through the relevant Privacy Notices. In some cases the processing of certain sensitive data may be necessary to operate

the Institution's policies, such as health and safety and equal opportunities. Where data is sensitive, for example information about health, race or gender, processing will only ever take place for legitimate business purposes. No other processing of sensitive data relating to the Institution's members will take place without express consent.

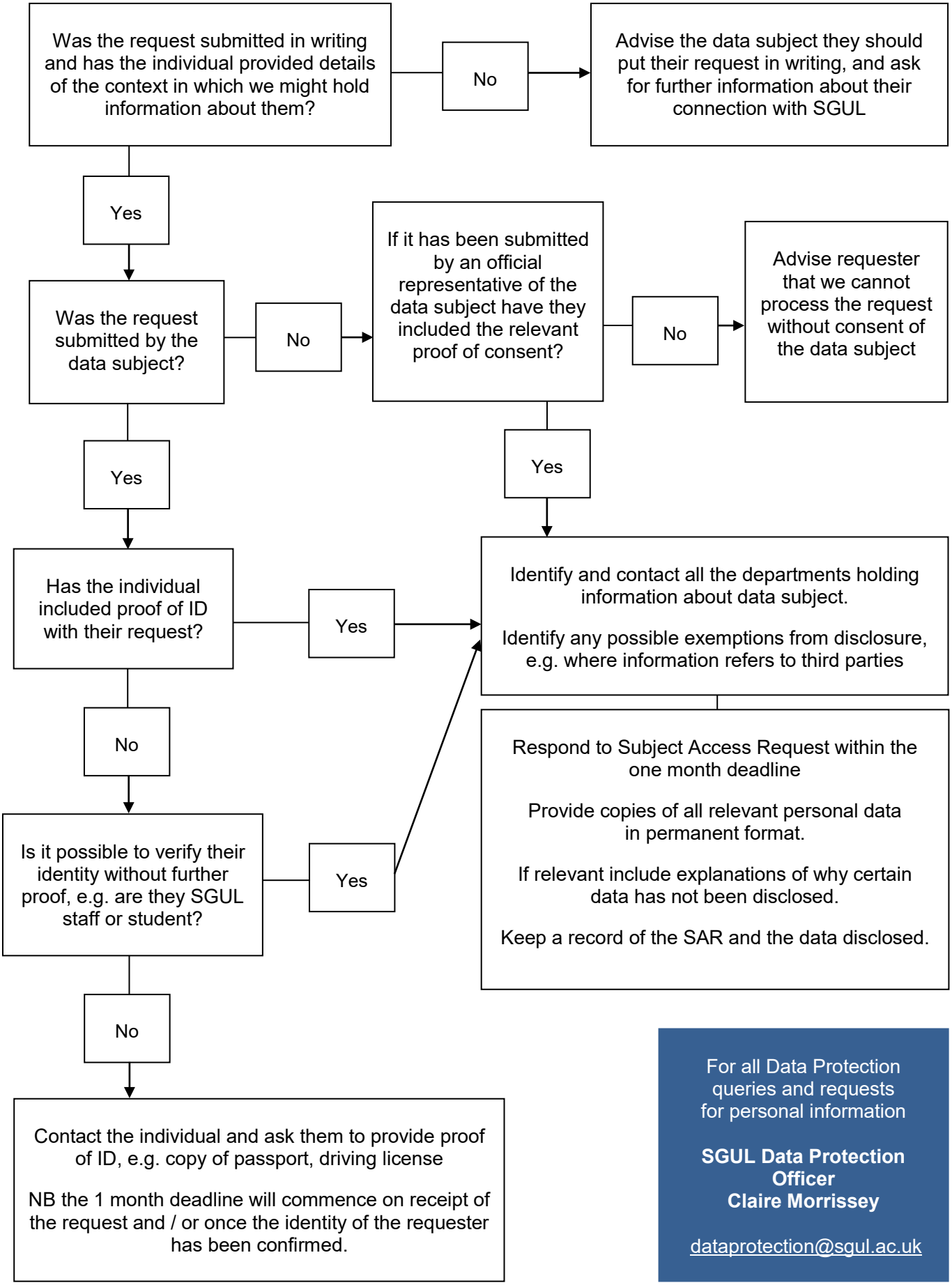
10. The Institution's designated Data Controller

The Institution is the data controller under Data Protection Legislation and is therefore ultimately responsible for implementation. However, day to day matters will be dealt with by the Data Protection Officer, details of which are below:

Claire Morrissey
Data Protection Officer

Tel: 020 8725 0668 Email: dataprotection@sgul.ac.uk

Appendix A
Process for responding to a Subject Access Request (SAR)



For all Data Protection queries and requests for personal information

SGUL Data Protection Officer
Claire Morrissey

dataprotection@sgul.ac.uk