**St George’s, University of London**

**Information Sharing Procedure**

1. **Purpose**
   1. This document sets out the procedure for information sharing agreements (ISA) for St George’s, University of London (SGUL) apart from information sharing which is part of a project managed by the Joint Research and Enterprise Services whose own procedures must be followed. The process governs the development of an ISA that are purpose specific and cover both: the regular supply of information; and one off supply of a large set of information.
   2. It applies to the whole of SGUL where there is a recognised need to share information with other organisations. If the ISA relates to personal data then all stages of the ISA must be completed. If the information does not include personal data (i.e. financial information, statistics), but the information is sensitive and warrants a protective marking, the ISA must be followed but the legal basis can be omitted.
2. **Roles and responsibilities:**
   1. The Information Governance Steering Group (IGSG) must approve all information sharing requests.
   2. Urgent ISAs can be approved by the Senior Information Risk Owner (SIRO) but must be presented at the next IGSG for comment.
3. **Approach** 
   1. All requests for sharing information with other organisations must be submitted to the Data Protection Officer (DPO) using the ISA form. The completed ISA form will identify the requirements for the sharing of information and define the key points of the arrangement, forming the basis for the information sharing agreement. The procedure requires managers to draw up a short business case and make recommendations for their Director level manager in their capacity as the Information Asset Owner (IAO) to endorse.
      1. The short business case, setting out the purpose of the ISA, must clearly define:

* those organisations or persons who are signatories to the sharing agreement
* the specific purposes for which information is to be shared;
* the legal gateway for sharing any information defined as personal or sensitive personal. This part establishes that the sharing has a statutory or common law basis and that sharing is compliant with current Data Privacy Laws. If personal data is shared the legal basis for the sharing must be established in any documented and formal agreement.
  + 1. In-depth guidance on completing an ISA can be found in the SGUL Information Sharing Guidance document.
  1. A Data Protection Impact Assessment (DPIA) must be carried out before information is shared and signed off by both organisations.
* The appropriate IAO, supported by the Data protection Officer, is responsible for carrying out the PDIA to ensure the requirements adhere to the appropriate legislation.
* The PDIA is informed by using the ‘Data Sharing Code of Practice’ and the data sharing checklists published by the Information Commissioners Office (ICO) as guidelines for person and personal sensitive information.

1. **Controls**
   1. The IGSG provide high level oversight in the management of ISAs.
   2. IAOs, via their Information Governance Leads, are responsible for ensuring compliance with this procedure when they or their teams are involved in an information sharing request.
   3. Information sharing can only occur when sanctioned by the IGSG or in exceptional circumstances by the SIRO.
2. **Assurance**
   1. A register of ISAs will be held by the DPO that will allow for the easy monitoring and reviewing of information sharing arrangements.
   2. An annual review of ISAs is carried out by respective IAOs with responsibility for the ISA who will report on any risks to the IGSG.
   3. Staff compliance with this procedure will be checked during audits arranged by the relevant Information Governance Lead.