#

# *Data Protection Impact Assessment – COVID-19*

# *Temporary usage on research projects in support of COVID-19 or running of our essential services during the outbreak*

This is a simplified Data Protection Impact Assessment (DPIA) that has been developed for use with urgent Data Protection / IT developments during the COVID-19 Coronavirus outbreak, so as to not delay the development / deployment of projects or processes in support of essential research or services during the pandemic. It has been designed to ensure rudimentary due diligence in line with Data Protection legislation, so as to capture and manage any immediate Data Protection concerns. It does not cover all elements required of a standard DPIA that would be used within a Business As Usual scenario. Consequently, **once the immediate pandemic situation has subsided, the Team implementing the project to which this DPIA relates will be required to complete a full retrospective DPIA**.

Note: University hosted video conferences / meetings are to be carried out by the use of Microsoft Teams or Teams Live. Due to recognised security concerns, we do not allow the use of other video conferencing services for St George’s hosted events without the permission of the Senior Information Risk Owner (siro@sgul.ac.uk).

Support in completing this form can be provided by the Information Governance Manager (Geoff Gray) or Data Protection Officer (Claire Morrissey)

**Step 1: Project Administration**

**Project Title:**

**Senior Responsible Person for the Project:**

Name:

Job Title:

Email:

Extension/Mobile Number:

**Step 2: Project Details**

2.1 What are the full details and rationale of the project?

2.2 What is the name of the system / application / process to be used?

2.3 Is the system / application / process being used in any similar organisation to SGUL, and if so, which? (See also Q3.5.)

**Step 3: Risk Assessment and Mitigation**

3.1 Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.*

3.2 Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*

3.3 Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*

3.4 Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?

3.5 If the answer is “Yes” to 3.1, 3.2, 3.3 or 3.4 how are these to be Reduced or Mitigated?

3.6 Once the mitigations in 3.5 are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** *(please tick)* | **x** | **Severity** *(please tick)* | **=** |  |
| **1** |  | Rare | **1** |  | Negligible |
| **2** |  | Unlikely | **2** |  | Minor |
| **3** |  | Possible | **3** |  | Moderate |
| **4** |  | Likely | **4** |  | Major |
| **5** |  | Almost certain | **5** |  | Catastrophic |

Any risks scoring above 6 will need to be reviewed by either the Senior Information Risk Owner (SIRO) – Rob Churm or the Deputy Senior Information Risk Owner (DSIRO) Paul Ratcliffe.

**Step 4: Project Sign-Off**

Sign-off can be given at Director level for any DPIAs scoring up to 6 in Q3.6, a copy of which must be emailed to the Data Protection Officer & Information Governance Manager. For those scoring above this it must be from the SGUL SIRO or Dep SIRO demonstrating that risks have been acknowledged and accepted for the duration of the pandemic, and will be added to the SGUL Information Risk Register.

Name:

Job Title:

Email:

Extension/Mobile Number: