**St Georges, University of London (SGUL)**

**Personal Data Breach Investigation Form**

This form must be completed in full by the relevant staff member as nominated by the Information Asset Owner.

The report should be submitted only once all actions relating to the breach have been completed and by the date specified by the Data Protection Officer.

|  |  |
| --- | --- |
| Name of investigation lead: |  |
| Date investigation started: |  | Date investigation completed: |  |
| Describe the incident: |  |

|  |
| --- |
| Assessment: |
| Note: Any significant breaches must be notified to the ICO within 72 hours. If you consider this to be a significant breach or require advice on this assessment then contact the SGUL Data Protection Officer as the earliest opportunity. |
| What type of data is involved? |  |
| How sensitive is it? | *Data is sensitive because of its very personal nature (name, address, health records) whilst other data types are sensitive because of what might happen if that information is misused (bank account details)* |
|  |
| If the data has been misplaced, lost or stolen, are there any protections in place such as encryption? |  |
| What has happened to the data?  |  |
| Regardless of what has happened to the data, what could the data tell a third party about the individual? | *Sensitive data could mean very little to an opportunistic laptop thief, whereas apparently trivial snippets of information could help a determined fraudster build up a detailed picture of someone* |
|  |
| How many individuals’ personal data are affected by the breach? |  |
| Who are the individual(s) whose data has been breached? | *You should not name the individual(s), instead you should provide a description of who they are and their relationship to the university, e.g. staff member, MBBS students, research study participants* |
|  |
|  |
| What harm can come to those individuals? | *Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life? If individuals’ bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.* |
|  |
| Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide? |  |
| Have staff involved received DPA training? | *Please also indicate how recently training was completed, e.g. what month/year* |
|  |
| If the breach involved contractors is data protection mentioned in the contract with them? |  |
| What action has been taken to mitigate or resolve the risks regarding the breach? |  |
| What lessons have been learned from the incident? |  |
| What actions have been taken to prevent a reoccurrence of the incident? |  |
| Chronology of events: | *(provide dates and times in sequence)* |
|  |