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

**Confidential Data Breach Investigation Form**

This form must be completed in full by the relevant staff member as nominated by the data owner.

The report should be submitted only once all actions relating to the breach have been completed.

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

|  |  |
| --- | --- |
| Assessment: | |
|  | |
| What type of data is involved? |  |
| How confidential is it? | *Data is confidential because of its sensitivity (research, financial and governance data all have different levels of sensitivity). Always refer to the data owner for advice.* |
|  |
| 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 workings of the university? | *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 a particular business activity or research project etc.* |
|  |
| What quantity of data is involved in the incident? | *(an entire research project, a whole database, a single file/document etc.)* |
|  |
| What physical, financial or reputational harm can come to the University, staff or students? |  |
| Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service the university provides? |  |
| Who is the individual(s) or organisation involved in the incident? |  |
| Have staff involved received Information Security Awareness training? | *Please also indicate how recently training was completed, e.g. what month/year* |
|  |
| If the incident involved contractors is confidentiality 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)* |
|  |