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

**Confidential Data Incident Reporting Procedure**

1. This procedure is to be followed in the event of a data incident involving University confidential data. If the incident does involve personal data then the Personal Data Incident Reporting Procedure must be followed. The University will ensure that confidential data it holds is protected and will take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to the data. This document provides guidance on actions to be taken by staff in the event of a confidential data security incident.
2. All staff have a responsibility to report any University data security incident they become aware of and where possible put in place immediate safeguards if discovering information is not protected.
3. The following are examples of confidential data incidents (and this is by no means exhaustive):
	* Loss of a device containing confidential data (especially if unencrypted);
	* Email containing confidential data sent to wrong email address;
	* Unauthorised access to confidential data such as research or financial data.
	* Destruction of confidential data (where no backup exists);
	* Document(s) containing confidential data on the MS 365 drive being shared to unauthorised people;
	* Confidential data viewed on people’s desks etc by unauthorised people;
	* University systems hacked and confidential data stolen/altered/destroyed
4. Possible confidential data security incident must be reported immediately to the Head of Information Governance (HIG) either by:
	* Completing the data incident reporting found on the Web page [information-technical-security](https://www.sgul.ac.uk/about/our-professional-services/information-services/information-governance/policies-and-procedures/information-technical-security) :or
	* emailing the HIG on IG@sgul.ac.uk;

Staff members must also notify their line manager of the incident.

1. All notified confidential data security incidents are logged by the HIG a Data Incident Reporting Form is sent to the staff member reporting the incident for them to complete and return immediately to the HIG if one not already raised.
2. The Line Manager is to assess the possible severity of the data incident and to take immediate action as appropriate to the incident to mitigate any further escalation of the incident.
3. The HIG will, depending on the severity of the incident, notify the relevant IAO who will assign a senior manager to investigate the incident on their behalf. The assigned officer will have 10 days to complete and report on the investigation back to the DPO.
4. If the incident is immediately classed as significant by the HIG then the SIRO will be informed along with the relevant IAO, Chief Operations Officer and Dir Legal Services.