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

**Personal Data Incident Reporting Procedure**

1. In accordance with the Data Protection Act 2018 (DPA 18) organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This document provides guidance on actions to be taken by staff in the event of a personal data security incident.
2. All staff have a responsibility to report any personal data security incident they become aware of and where possible put in place immediate safeguards if discovering personal information that is not protected.
3. The following are examples of personal data incidents (and this is by no means exhaustive):
   * Loss of a device containing personal data (especially if unencrypted);
   * Email containing personal data sent to wrong email address;
   * Unauthorised access to SITS (or any other personal data system);
   * Destruction of personal information in a fire (where no backup exists);
   * Document(s) on the MS 365 drive being shared to unauthorised people;
   * Personal data viewed on peoples desks etc by unauthorised people;
   * University systems hacked and personal data stolen/altered/destroyed
4. Possible data security incident must be reported immediately to the SGUL Data Protection Officer (DPO) 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 DPO on [dataprotection@sgul.ac.uk](mailto:dataprotection@sgul.ac.uk);

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

1. All notified data security incidents are logged by the DPO and a Data Incident Reporting Form is sent to the staff member reporting the incident for them to complete and return immediately to the DPO.
2. Depending on the possible severity of the data incident the notified Line Manager is take immediate action as appropriate to the incident to mitigate any further escalation of the incident.
3. The DPO 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 DPO then the SIRO, relevant IAO, Chief Operations Officer, Dir Legal Services and Information Governance Manager will be informed immediately. As significant incidents must be notified to the ICO within 72 hours a decision on further actions will then be considered by this group.
5. The final decision of notifying the ICO will be made by the SIRO.