St George's, University of London

Clear Desk and Screen Procedure

1 Introduction

1.1 The overall purpose of this procedure is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them.

2 Responsibility

2.1 This procedure applies to everyone who has access to SGUL's information, information assets or IT equipment, whether office based or working remotely.

2.2 All Directors in their capacity as Information Asset Owners (IAOs) are responsible for ensuring compliance with this procedure.

3 Actions

3.1 Clear Desk:

- All users are to leave their desk/workstation free of sensitive or confidential paper at the end of the day or when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.
- Consideration should be given to the protective marking and sensitivity of information when storing it.
- Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets.
- Other documents may be locked in storage that SGUL provides individual staff members.
- All office managers will have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.
- Users should make sure that any documents lying on their desk/workstation are not visible to visitors, members of the public or colleagues who are not authorised to see them.
- Sensitive information, when printed, should be cleared from printers immediately.

3.2 Clear Screen:

- All users are expected to log off from their PCs/ laptops when left for long periods and overnight.

- When leaving their computer unattended users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation or the Windows key + L. The SGUL's IT system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.
- Mobile devices through which access to the network can be obtained, for example tablets, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use.
- Users should make sure that no open documents on their computer screens are visible to visitors, members of the public or colleagues who are not authorised to view them.

4 Compliance

4.1 The SGUL security team will include checks for non-compliance with the procedure in their scheduled patrols. The security team will issue a 'warning' card where they have observed a failure to adhere to either the clear desk or clear screen procedure. Where a staff member has been issued with their third warning, the Data Protection Officer will be notified and the staff member will be required to re-take the online data security training.

4.2 Monitoring of compliance with this procedure will also form part of the monthly reviews carried out by IG Leads within their respective divisions.

4.3 Any concerns regarding compliance with this procedure should be directed to the Data Protection Officer. Serious data security incidents must be reported direct to either the Senior Information Risk Owner (SIRO) or the Data Protection Officer.

5 Assurance

5.1 The DPO will inform the IGSG, chaired by the SIRO, of all information breaches and make recommendations on those which should be notified to the Executive Board.