Protecting Personal Data while Working Remotely

This policy outlines procedures for working from home or travelling for business. Many Kings staff routinely work from home or take work home, many staff also travel for business, whether overseas or between various company locations. This document details the measures to be taken to protect personal data in addition to the protections detailed in the Data Protection Policy and associated documents, particularly those dealing with printed materials and the sharing of electronic data.

General Principles

A number of general principles apply, regardless of the situation in which data is accessed, held or taken off-site. Some of these points are also included in other policy documents.

- Laptops and mobile devices must be encrypted and password-protected
- Laptops and mobile devices must be installed with up-to-date operating systems and security software
- Personal data, wherever possible, should be held and accessed remotely via a secure server or cloud storage service
- Only cloud storage services provided by Kings should be used for storing and accessing personal data
- Wherever possible, USB sticks and similar easily lost data storage devices should not be used to store or transport personal data, seek alternative secure methods of making data available where it is needed

Home Workers

Home workers routinely access data away from an official Kings site or workplace and need to ensure the following:

- Where personal data is printed or stored in paper format, such as in notebooks, it must be stored in a lockable cupboard, with the keys stored securely and separately
- A clear desk policy is observed, taking care to ensure that printed or electronic data cannot be accessed by family members, visitors to the home or intruders
- Laptops and other devices are locked while unattended
- All data is kept in line with Kings Data Retention Policy and destroyed and disposed of securely after its retention period. For printed materials, this means taking the documentation to a school or office site for shredding or shredding it using an appropriate home shredder. Printed personal data must not be disposed of alongside normal rubbish.
- Where information is transported between the home and a Kings site, it must be done so securely, in line with the guidance on Travelling for Business below

Taking Work Home

Staff employed by Kings often take work home, for example for marking, report writing, managing the emergency phone, etc. To ensure this data is protected, the following needs to be ensured:

- Personal data is accessed remotely as much as possible, via a secure server or cloud service
- Any printed personal data taken off-site should be signed out by the staff member's line manager and, if appropriate, signed back in on return to the place of work
- While personal data is off-site it should be protected as much as possible. Work laptops and devices should be locked while unattended, paper records should be stored securely and away from family members, visitors to the home and intruders
- While in transit, data should be stored securely, such as in a zipped, secured bag, out of sight and remaining in the possession of the staff member at all times. Documents and devices should not be left unattended in cars, on public transport or in areas where they may easily be lost or stolen
- Personal data should never be disposed of alongside normal rubbish
- Personal data should never be stored in the home, unless the staff member is a homeworker and is authorised to do so

Travelling for Business

Kings has a number of staff who travel for work on a routine basis, whether overseas or between various company locations.

Whilst travelling for work the following needs to be ensured:

- While in transit, data should be stored securely, such as in a zipped, secured bag, out of sight and in the possession of the staff member at all times. Documents and devices should not be left unattended in cars, on public transport or in areas where they may easily be lost or stolen
- Staff should not transport any personal data in luggage which will leave their possession, such as in hold luggage on an aeroplane or coach
- Staff should be conscious of being overlooked whilst travelling, such as when working on a train, aeroplane or in a café, and should not view personal data if there is a risk of this
- Printed personal data should be kept until it can be destroyed securely, it should never be disposed of alongside normal rubbish