Addendum to Mobile Working Policy

Introduction

In certain circumstances it will be necessary for staff to work from home, possibly for long periods of time. This addendum sets out the security levels required to maintain the confidentiality and security of data outside of the office environment.

There are more risks to information and equipment associated with remote working than being in the office. Even in special circumstances you must follow UK Data Protection Legislation whilst working remotely.

Your Responsibilities

You are responsible for the security of your equipment and information when you are working from home, you need to adhere to the below:

- When taking information or equipment home with you, or returning it, make sure it is kept out of sight at all times, for example in a bag that can be secured by a zip or button fastening. If traveling in a car bags should be stored out of sight. If traveling on public transport ensure you keep any equipment and/or records on your person at all times.

- Only use approved equipment – the laptops issued by the CCG

- Work equipment should be set up in an area where you have some privacy to handle calls and emails that may involve the processing and/or handling of a patient's health information.

- Make sure that any patient information is not viewed or overheard by anyone else in your home. You can do this by ensuring that other members of the household are not able to access your work equipment when in use. Always lock your screen when you are away from your laptop.

- If making notes please use your laptop to do this where possible rather than a paper notepad.

- Place all work documents and/ or paper records out of sight when not in use, where possible in a secure lockable bag or storage unit. If you have any paper documents or notes these should be stored separately to your laptop.

- Where you have created any new information in paper ensure when possible it is transferred to the appropriate electronic system and any paper copies are disposed of in confidential waste bins in the office at the earliest opportunity. Do not dispose of any personal data at home

.

Communication tools
Where it is not possible to meet with colleagues or patients, alternative methods of communication are required. Wherever possible Skype or Microsoft Teams should be used, however it is recognised that this may not be accessible to all. It has therefore been agreed that other methods such as WhatsApp may be used.

Your Responsibilities
Any staff member using alternative communication tools for business purposes must follow the below rules. This applies to any information that is created or received as part of a CCG task, be that communication between teams on work matters, contacting your manager or service delivery.

Before use please ensure:

- you only use alternative communication tools after consulting with your line manager or if in doubt the Information Governance team.
- alternative communication tools are only used where the CCG recommended options are not available and it is critical to service delivery.

While using please ensure:

- Any correspondence created for business purposes is kept separate from any personal conversations that you have. You can do this by creating a new group and adding any relevant officers or partners to it.
- Where possible you should avoid using any alternative to send personal or sensitive data. However, should this be a necessity you will be allowed to do so but you should ensure that you provide only the minimum amount of information needed.

After using please ensure:

- If a conversation contains any decision-making, employee or patient data it should be exported from application and uploaded to the relevant filing system on the Network.
- Once a conversation is no longer required, all parties in the conversation must clear chat / clear messages to remove all versions of it from every device.

Responding to Information Requests
In carrying out CCG business please be aware that any information, even that stored on external applications, is subject to statutory information requests that the CCG may receive such as Freedom of Information requests or Subject Access Requests. This includes:

- any messages between you and your staff,
- <u>any correspondence you created from a personal mobile number for work purpose</u>.