Remote working policy

Part of the NASGP Locum Toolkit

Name of GP	
Policy date	
Review date	

Business continuity

- ❏ Although I can't be held responsible for any technical failures to do with services beyond my control such as remote desktops, VPNs or clinical IT systems, if such a situation occurs, I will contact the practice to arrange alternative means to provide immediate cover.

Device and software security

For example:

- ❏ I accept full responsibility for the security and safety of any devices used for remote working.
- ❏ I will not leave the device unattended for any reason whilst working on it unless the session is 'locked'.
- ❏ Any devices used will have full antivirus and malware software and this will be kept updated.
- ❏ Any devices used have in-built hard disk encryption.
- ❏ Biometrics such as fingerprint and facial recognition will be used wherever possible.
- ❏ All passwords used on any devices controlled by me will comply with recommendations from the National Cyber Security Centre https://www.ncsc.gov.uk/collection/passwords.
- ❏ Multi-factor authentication will be used wherever possible.
- ❏ Only approved NHS applications to access patient data will be used
- ❏ No patient identifiable information will be stored on the hard drive.

Data security

For example:

- ❏ No other people will be given access to the device.
- ❏ I will access your practice's cloud system, and thereby patient data, in line with GDPR principles i.e. intended use for direct provision of clinical care or for ongoing clinical governance related to clinical care. Examples of clinical governance may be for purposes of complaint, compliments, quality assurance activities.
- ❏ Where appropriate, if using a VPN, access to NHS software will only be via VPN.
- ❏ The VPN will be connected using private Wifi only which will not have a default password and username.