# Working From Home
## Use of Personal Devices

In response to the COVID-19 pandemic, the rules on the use of personal devices for work purposes has been relaxed so that some systems like NHS Mail , NHS Near Me and Office 365 may be accessed. However, all reasonable steps still need to be taken to keep devices, systems and data secure.

### ENSURE PRIVACY
If possible, try to work in an area where you will have total privacy.  Can your screen or paperwork be shielded from view from others in your household?

### DEVICE SECURITY
Enable any security features on your device. This includes encryption, passwords, PIN numbers or biometric features such as fingerprint or facial recognition.

### SOFTWARE UPDATES
Devices should be fully updated with the latest security updates and patches.

### ANTI-VIRUS SOFTWARE
Laptops and desktops  should have anti-virus software installed and should be set to automatically update.


### PERSONAL USE
Where possible, do not mix work and personal useage on your personal device. Sharing of personal devices which are being used for work purposes should be avoided.

### DOWNLOAD NHS DATA
Avoid downloading NHS data  on to personal devices especially where it is of a confidential nature. If it is absolutely necessary, the data should be deleted as soon as possible.

### CLOUD STORAGE
Do not upload NHS data to store or share in commercial cloud storage solutions such as Dropbox and Google Drive. Only NHS Highland cloud systems should be used.

### FURTHER INFORMATION
For further support contact the Information Assurance & IT Security team by emailing high-uhb.informationsecurity@nhs.net