Mobile Devices and Bring Your Own Device (BYOD) – Office Teams

- The use of a **personally owned mobile device** to connect to the Lifestyle by Homecare Services network is a privilege granted to employees only upon formal approval of IT Management.
- All **personally owned** laptops and/or workstations must have approved virus and spyware detection/protection software, along with personal firewall protection active.
- Mobile devices that access Lifestyle by Homecare Services email must have a PIN or other authentication mechanism enabled.
- **Confidential information** should only be stored on devices that are encrypted in compliance with the Lifestyle by Homecare Services Encryption Standard.
- Lifestyle by Homecare Services **confidential information** should not be stored on any personally owned **mobile device**. Where it is necessary to use your device to send confidential information – for example to GP surgeries or the office, this should be deleted from your device straight away. No information should be automatically saved to your gallery or back up storage options such as icloud; google drive or one drive.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to Lifestyle by Homecare Services management immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Rooted or jailbroken** devices should not be used to connect to Lifestyle by Homecare Services **Information Resources**.
- Lifestyle by Homecare Services IT Management may choose to execute "**remote wipe**" capabilities for **mobile devices** without warning (see Mobile Device Email Acknowledgement).
- If there is a suspected **incident** or breach associated with a **mobile device**, it may be necessary to remove the device from the personnel's possession as part of a formal investigation.
- All mobile device usage in relation to Lifestyle by Homecare Services **Information Resources** may be monitored, at the discretion of Lifestyle by Homecare Services IT Management.
- Lifestyle by Homecare Services IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Lifestyle by Homecare Services IT support may not assist in troubleshooting device usability issues.
- Lifestyle by Homecare Services reserves the right to revoke **personally owned mobile device** use privileges if personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on company time or using Lifestyle by Homecare Services resources. Only hands-free talking while driving is permitted, while on company time or when using Lifestyle by Homecare Services resources.
- Use of **personally owned** devices must comply with all other Lifestyle by Homecare Services policies.

Mobile Devices and Bring Your Own Device (BYOD) – Community Teams

- The use of a **personally owned mobile device** to connect to the Lifestyle by Homecare Services network is a privilege granted to employees only upon formal approval of IT Management.
- **Confidential information** should only be stored on devices that are encrypted in compliance with the Lifestyle by Homecare Services Encryption Standard.

- Lifestyle by Homecare Services **confidential information** should not be stored on any personally owned **mobile device**. Where it is necessary to use your device to send confidential information – for example to GP surgeries or the office, this should be deleted from your device straight away. No information should be automatically saved to your gallery or back up storage options such as icloud; google drive or one drive.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to Lifestyle by Homecare Services management immediately.
- All **mobile devices** must maintain up-to-date versions of all software and applications.
- All personnel are expected to use **mobile devices** in an ethical manner.
- **Rooted or jailbroken** devices should not be used to connect to Lifestyle by Homecare Services **Information Resources**.
- Lifestyle by Homecare Services IT support for **personally owned mobile devices** is limited to assistance in complying with this policy. Lifestyle by Homecare Services IT support may not assist in troubleshooting device usability issues.
- Texting or emailing while driving is not permitted while on company time or using Lifestyle by Homecare Services resources. Only hands-free talking while driving is permitted, while on company time or when using Lifestyle by Homecare Services resources.
- Use of **personally owned** devices must comply with all other Lifestyle by Homecare Services policies.

Do's and Don't – Office and Community Teams

Do	Don't
Keep your passwords secure	Don't share your device or passwords
Use biometric features to secure the device if possible	Don't make copies of data or take screenshots
Make use of multi-factor authentication	Don't access systems without authorisation
Keep your operating system updated	Don't save work in unapproved locations or applications
Be careful who can see your screen when accessing work systems	Don't share data without approval
Consider using 'Find my device' and global positioning system (GPS) features if these are available on the device to help in the event of device loss	Don't save any confidential information on your device or back up storage
Report lost or stolen devices	Don't use 'remember me' functions on any work-related applications or platforms
Be aware of your responsibility for all costs	
Facilitate IT to conduct spot checks if required	
Inform IT if you leave employment with the organisation	
Use different passwords for your work applications than your personal passwords	
Avoid reusing passwords or using the same password for multiple platforms/applications	