Device Security Policy

Healthwatch Derbyshire purchases employee's smartphones and tablets/laptops necessary for their work. Healthwatch Derbyshire reserves the right to revoke this privilege if users do not abide by the procedures outlined in this policy.

This policy is intended to protect the security and integrity of Healthwatch Derbyshire's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Healthwatch Derbyshire employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

Healthwatch Derbyshire defines acceptable use as activities that directly or indirectly support the business of Healthwatch Derbyshire.

Healthwatch Derbyshire has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted. Additionally, only factory-fitted or fixed Satellite Navigation devices are to be used whilst driving, additionally mobile phones can be used for navigation purposes.

However, in order to operate/programme any of the above devices the vehicle must be safely pulled over to the side of the road. Where mobile phones are being used, the vehicle must also be switched off.

Devices and Support

Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.

Tablets including iPad and Android are allowed.

Connectivity issues are supported by IT; employees should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device, and a strong password is required to access the company network
- The company's strong password policy is: *Passwords must be at least six characters and a combination of upper-and lower-case letters, numbers. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords*
- The device must lock itself with a password or PIN if it's idle for five minutes
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps
- Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network

- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the networks
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While Healthwatch Derbyshire will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts etc
- The company reserves the right to disconnect devices or disable services without notification
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying the communications officer or IT support immediately upon loss of a device
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above
- The employee is personally liable for all costs associated their device where their own personal equipment is used
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable (only applicable on personal devices
- Healthwatch Derbyshire reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Policy adopted on 10 August, 2020 and reviewed in August 2021,

Signature of the chair:

Date: 10.08.2021

This policy is next due for review on August 2022