Protective Marking: Official

DIGITAL POLICING PORTFOLIO

Frontline Digital Mobility National Guidelines

Portable Hotspots

March 2020

FRONTLINE DIGITAL MOBILITY

Important notice:

Frontline Digital Mobility (FDM) Programme Disclaimer

This document, and all referenced documents, have been prepared by or on behalf of the Digital Policing Portfolio (DPP) for the benefit of all police bodies, forces and agencies within the UK criminal justice system (Police Bodies) who are involved in the DPP.

The information contained in this document has been compiled by or on behalf of the DPP and may include material obtained from various sources which have not been verified or audited. This document also contains material proprietary to the DPP. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of the DPP or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document.

[Sussex Police and Crime Commissioner of Sackville House, Brooks Close, Lewes, East Sussex BN7 2FZ is the contracting party acting on behalf of the DPP.]

CLASSIFICATION, APPROVAL AND CIRCULATION

CLASSIFICATION

Government Security classification:	Official
Disclosable under FOIA 2000	Yes

APPROVAL

Name and role	Organisation
Dr Natalie Benton	FDM Programme Lead

CIRCULATION

Document Reference	FDM National Guidelines - Portable Hotspots
Version	Final
Last updated	11.03.20
Suggested review date	October 2020
Owner	FDM Programme Lead
Approval by	FDM Programme Lead

CONTENTS

1. Context

Frontline officers and staff need secure internet connectivity on their mobile devices in order to achieve remote access to their force systems and to be able to exchange data. The move towards greater mobile working is likely to increase this need, as officers and staff become more reliant on their mobile devices.

Frontline officers and staff often have more than one mobile device, e.g. a smartphone and a tablet or laptop. Mobile devices with inbuilt data connections are typically more expensive to purchase than their Wi-Fi only counterparts. Moreover, they have ongoing data costs also. Hotspots provide a crucial means of sharing data connections with multiple devices.

Portable hotspots are typically more reliable and faster than mobile device based hotspots, e.g. smartphone hotspots. In addition tethering from one mobile device to another (say a smartphone with cellular data to a Wi-Fi only tablet) rapidly drains the battery of the device with cellular data. Portable hotspots present the opportunity for forces to purchase Wi-Fi only mobile devices supported by portable hotspots, which could be shared by a team. However, there is of course a cost associated with the purchase of portable hotspots as well as ongoing data charges. Additionally, this would add to the number of peripherals an officer or staff member would need to carry on their body as well as adding to the number of peripherals managed by a force's IT department. Therefore, forces need to consider the opportunities and limitations of using portable hotpots depending on the use case for which they are intended.

Some forces have in-vehicle 4G routers, which broadcast their own Wi-Fi network, allowing devices to connect to the force's internal network. Portable hotspots are best suited to forces that do not currently have in-vehicle Wi-Fi routers or that have frontline officers and staff who patrol on foot, bicycle or are typically away from a vehicle. This could become a more frequent requirement with a continued focus to see frontline officers and staff both out of the station and visible to the public.

Portable hotspots can support cross-team collaboration, for example a team of Police Community Support Officers (PCSOs) who do not have force network connected devices, working together for a brief period to complete a specific engagement. Portable hotspots can also support more effective streaming of data. A portable hotspot could be used, for example, by Territorial / Tactical units that need to operate in a remote environment (e.g. at a large outdoor protest) to collect a lot of data through Wi-Fi enabled Body Worn Video footage that needs to be transferred to force systems. Ordinarily the unit would be required to return to a base to download the data, however, a portable hotspot could utilise cellular connectivity to stream from the scene. Wi-Fi dongles, which are typically used to provide data connectivity to laptops and PCs, are out of scope in this guideline, since they can only connect to one device at a time and connect via a full size USB port (which smartphones and tablets do not have).

Portable hotspots are a tried and tested peripheral. Advances continue to make them faster, better and smaller. There are many types of portable hotspots available in the market place with many variances in terms of specification, features and of course price. This guideline explores these variances and makes recommendations (see section *4. Recommendations,* page 3) to help forces make informed selections to accelerate their mobility maturity.

This guideline has been developed to reflect existing technology and related capabilities available in the market place to forces today. Consequently, this guideline does not currently reflect any future capabilities that may be delivered, for example, by other national programmes such as ESN or NLEDS. This guideline should be considered alongside force mobility strategies and future plans for ESN (for more information contact your regional ESN coordination manager).

2. An Introduction to the technology

2.1 Portable hotspots

A portable hotspot is a small pocket sized router, incorporating a data SIM, which can be used to access the internet on a variety of devices while on the move. Portable hotspots rely on cellular data to provide 3G, 4G and/or 5G internet access. Multiple devices can simultaneously share the connection of a single portable hotspot that is within range of their signal, approximately 20m indoors with a greater range outdoors. Some portable hotspot devices allow connection to 10 or more devices. This is likely to cost much less than paying for a mobile data plan for each of those mobile devices.

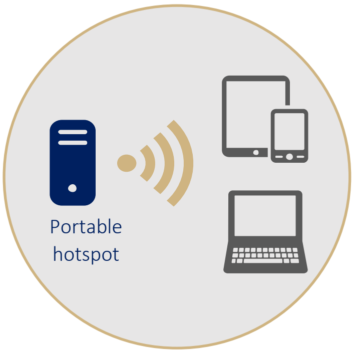

Figure 1

3. Benefits

Portable Hotspots offer a range of benefits for frontline mobility enablement. These are detailed below.

BENEFIT 01
LOW COST
A low price point peripheral to purchase.

BENEFIT 02
PORTABLE
A portable peripheral that can be used outside of police stations, further enabling frontline mobility.

BENEFIT 03
DEVICE AGNOSTIC
Portable hotspots can be used with a range of devices such as smartphones, tablets, and laptops.

BENEFIT 04
LOW MAINTENANCE
Requires little to no maintenance.

BENEFIT 05
MULTIPLE DEVICES
Portable hotspots are able to provide internet connection to multiple devices simultaneously.

BENEFIT 06
INCREASED SPEED
Portable hotspots provide a way of adding 4G connectivity to older 3G only devices.

BENEFIT 07
BATTERY LIFE
Using a portable hotspot instead of tethering from another mobile device conserves the ‘slave’ mobile device’s battery.

BENEFIT 08
Wi-Fi ONLY DEVICES
Portable hotspots provides remote internet access to Wi-Fi only devices.

Figure 2

4. Recommendations

A defined list of guidelines have been established and detailed below.

Guideline ID	Recommendations	Section Reference	Guideline Theme
GL-PH-01	It is recommended that forces considering purchasing portable hotspots, purchase ones capable of supporting several devices at once, to allow sharing across teams.	6.1.1 Portable hotspot connections	Availability
GL-PH-02	It is recommended that forces compare network service providers' coverage in their force area when selecting a portable hotspot.	6.2 Network service providers	
GL-PH-03	A recommended target price range for a 4G LTE portable hotspot is £60 to £80. Due to the way in which portable hotspots would be used on the frontline and coupled with the fact many forces consulted do not repair damaged low cost peripherals, portable hotspots above this price range are considered unlikely to deliver best value for money. Forces are recommended to explore bulk purchasing portable hotspots, which could reduce down the price per unit cost. Purchasing through a network provider often means users get the device itself for free, depending on the data plan contract. If a force is purchasing a dual portable hotspot and power bank, a recommended target price is up to £120.	6.7 Price	Cost
GL-PH-04	If a portable hotspot is to be shared by a team of officers/staff, it is probable that its rechargeable lithium battery could degrade relatively quickly. It is recommended that forces therefore consider portable hotspots with user-replaceable rechargeable batteries so that the lifespan of the device can be extended.	6.3.1 Battery Type	Durability
GL-PH-05	It is recommended that if replacing a portable hotspot battery, forces purchase Original Equipment Manufacturer (OEM) batteries to ensure the battery quality.	6.3.1 Battery Type	
GL-PH-06	It is recommended that forces select 4G LTE-Advanced enabled portable hotspots as they are fast, tried and tested and offer good geographic coverage.	6.1 Cellular network types	Performance
GL-PH-07	It is recommended that forces select portable hotspots that support 5GHz Wi-Fi to provide faster speeds, a stronger signal and a more stable connection.	6.1 Cellular network types	

Guideline ID	Recommendations	Section Reference	Guideline Theme
GL-PH-08	A portable hotspot with a battery capacity of around 3000mAh or higher is recommended to ensure that it can provide connection to multiple devices over a full 12-hour shift.	6.3.2 Battery capacity	**Performance**
GL-PH-09	While forces could benefit from having ruggedised portable hotspots, they do tend to be heavier and more expensive. Given that forces report that when selecting cheaper peripherals they are less concerned about damage it is recommended that that additional expense and weight is spared and non-ruggedised portable hotspots are selected.	6.6.3 Ruggedisation	**Ruggedisation and Environmental proofing**
GL-PH-10	High quality charging cables are recommended, since they offer more protection from possible power surges and overheating, which can damage connected devices. Additionally, they reduce the risk of cable failure, which could result in officers/staff being unable to use the portable hotspot.	6.3.3 Charging ports and cables	**Safety/ Security**
GL-PH-11	It is recommended that forces use a VPN when using a portable hotspot to provide internet access.	6.4.1 VPN	
GL-PH-12	It is recommended that Wi-Fi Protected Access II (WPA2) is enabled as the encryption type for portable hotspots as it is current, widely used and proven to be secure.	6.4.2 WPA-PSK	
GL-PH-13	It is recommended that forces change the SSID, the portable hotspot's network name, from the default to something random, avoiding dictionary words. It is also recommended that the SSID is set to non-visible on portable hotspots.	6.4.3 SSID and password	
GL-PH-14	It is recommended that forces change the wireless network password (known as the pre-shared key). Forces should follow National Cyber Security Centre (NCSC) guidance on password policies.	6.4.3 SSID and password	
GL-PH-15	It is recommended that where available, forces adopt a “deny all” policy to TCP/UDP ports and only open ports necessary for their specific use case for example 1194 for VPN and 443 for https.	6.4.4 Port filtering	
GL-PH-16	It is recommended that forces avoid purchasing portable hotspots with micro SD card slots, or that if these exist, they are disabled, in order to mitigate data security risks.	6.6.2 Data storage capability	

Guideline ID	Recommendations	Section Reference	Guideline Theme
GL-PH-17	It is recommended that forces select a portable hotspot with a port/cable arrangement that is the same as other force devices in order to simplify and reduce the number of chargers and charging cables required.	6.3.3 Charging ports and cables	Usability
GL-PH-18	To ensure the portable hotspot does not add burdensome weight to what officers and staff already need as "personal carry", it is recommended for hotspots to weigh no more than 250 grams. To ensure the portable hotspot can fit comfortably into uniform pockets, it is also recommended that it is no larger than 15cm x 10cm x 2cm.	6.5 Size and weight	
GL-PH-19	Forces that need both portable power banks and portable hotspots are recommended to consider the purchase of dual purpose portable hotspots with portable power bank capability, as this will reduce the number of peripherals required.	6.6.1 Dual purpose portable hotspot	
GL-PH-20	While forces could benefit from having portable hotspots with LCD displays, they do tend to be more expensive. It is recommended that that additional expense is spared and portable hotspots without LCD displays are selected.	6.6.4 Display	

Table 1

5. Market place

5.1 Technology maturity

Portable hotspots are in use across police forces nationally. They are a tried and tested technology and today there is a competitive portable hotspot market with many different suppliers and specifications and features available.

6. Technology specification and features

6.1 Cellular network types

A portable hotspot utilises one or more of 3G, 4G or 5G cellular networks. The speed of the internet connection depends on the generation of cellular technology and the signal strength. Typically the later the generation, the faster the connection. When multiple mobile devices use the same portable hotspot, the connection speed can reduce.

3G, the third generation of wireless network technology, provides speeds of up to 21 Mbit/s for downloads and 5 Mbit/s for uploads. 4G LTE-Advanced offers faster download speeds of up to 300 Mbit/s.

5G is the latest generation of mobile internet, offering speeds that are faster than 4G data connections. However, 5G is still in its infancy, with limited geographic coverage particularly in rural areas. There are not yet many 5G mobile hotspots available on the market and those that are available are above the recommended price range for forces.

Some portable hotspots allow the user to switch between 3G, 4G or 5G or use a combination.

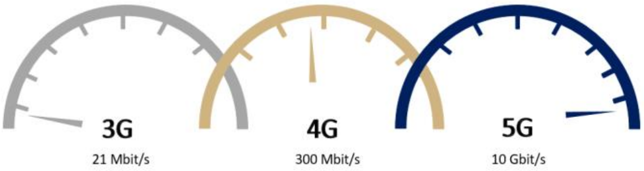

Figure 3

Portable hotspots support Wi-Fi operating in either the 2.4GHz band, 5GHz band or both 2.4GHz and 5GHz (dual-band).

Further information about the different cellular networks and Wi-Fi frequency bands can be found in *FDM's Connection Types guideline*.

It is recommended that forces select 4G LTE-Advanced enabled portable hotspots as they are fast, tried and tested and offer good geographic coverage.

It is recommended that forces select portable hotspots that support 5GHz Wi-Fi to provide faster speeds, a stronger signal and a more stable connection.

6.1.1 Portable hotspot connections

Portable hotspots can be connected to Wi-Fi-only devices (i.e. devices that do not have their own cellular capability and SIM). A tablet, for example, with mobile data support and a 4G data connection is typically around £100 more expensive than the same Wi-Fi only tablet. In addition, tablets with mobile data support also require ongoing data service charges. Tablet handset costs and ongoing data costs could both be reduced by using a single portable hotspot shared across multiple Wi-Fi only devices.

Figure 4

A portable hotspot can also provide a way of adding 4G connectivity to a 3G device. For example if an older smartphone is in use that does not support 4G networks, a 4G portable hotspot can be used to speed up its mobile internet connection.

There is a limit to the number of mobile devices that can be connected to a portable hotspot. Those designed for 3G networks typically can only support two or three mobile devices at once, while 4G LTE-Advanced and 5G portable hotspots can support 10 or more. All Wi-Fi enabled devices are compatible with portable hotspots.

It is recommended that forces considering purchasing portable hotspots, purchase ones capable of supporting several devices at once, to allow sharing across teams.

6.2 Network service providers

Portable hotspots are available from all major mobile network service providers, such as O2, EE, Three, and Vodafone. Portable hotspots can be purchased as "locked" or "unlocked", similar to smartphones. A locked portable hotspot is tied to a single network service provider and is not compatible with other network service provider's SIM cards. The major network service providers usually provide locked portable hotspots. An unlocked portable hotspot is not tied to a single network service provider and requires that a data-only SIM card be purchased separately. It is possible to unlock a locked portable hotspot, but there is a cost associated with this.

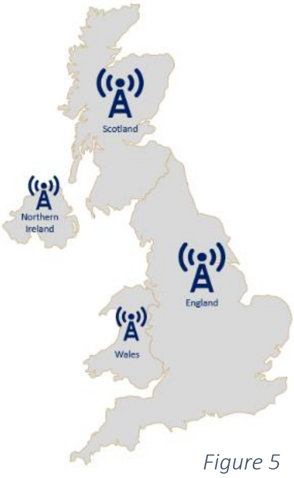

Figure 5

Network service providers typically offer one, 12, 18 or 24 month contracts. Longer contracts can result in the initial portable hotspot cost being zero or very low. Forces should consider bulk purchasing portable hotspots with a group data plan.

Network service providers deliver different network coverage levels across the country dependent on where their masts are situated. If there is no cellular connection, then the portable hotspot cannot provide any internet connection. This is no different to smartphone coverage.

It is recommended that forces compare network service providers' coverage in their force area when selecting a portable hotspot.

6.3 Power source

6.3.1 Battery type

Portable hotspots usually use one of two types of lithium batteries: Lithium-Ion or Lithium-Polymer. Both types have a long life expectancy and typically can carry out 500 charge/discharge cycles equating to, on average, a three-year lifespan. Over time, however, all lithium rechargeable batteries suffer from stress-induced ageing. Typically, a battery will lose 20% or more of its capacity after 1,000 charge cycles.

Many portable hotspots have a user-replaceable battery, which is easy to replace at the end of its lifespan. Replacement batteries can be purchased directly from portable hotspot manufacturers or via other companies. An Original Equipment Manufacturer (OEM) battery is identical to the original battery supplied with the portable hotpot. A non-OEM battery is made by another company and is invariably cheaper but often does not meet the same specifications in terms of capacity and durability.

If a portable hotspot is to be shared by a team of officers/staff, it is probable that its rechargeable lithium battery could degrade relatively quickly. It is recommended that forces therefore consider portable hotspots with user-replaceable rechargeable batteries so that the lifespan of the device can be extended.

It is recommended that if replacing a portable hotspot battery, forces purchase Original Equipment Manufacturer (OEM) batteries to maintain the battery quality.

6.3.2 Battery capacity

Lithium batteries are available with different capacities. Capacity is measured in mAh (milliamp hours) which denotes the capacity for power flow over time. Battery capacity for portable hotspots usually ranges from around 2000mAh to 6400mAh. According to manufacturers a 2000mAh battery can allow for up to eight hours of use while a 6400mAh battery can allow for up to 24 hours of use. The exact battery life of a portable hotspot is dependent on the amount of data usage as the more data that is consumed the quicker the battery will drain.

A portable hotspot with a battery capacity of around 3000mAh or higher is recommended to ensure that it can provide connection to multiple devices over a full 12-hour shift.

6.3.3 Charging ports and cables

Portable hotspots have input ports which are used to charge the portable hotspot from a mains electricity supply using connecting cables. Many portable hotspots have a Micro-USB port and are charged via a Micro-USB cable. However some newer models have a USB-C port and are charged via a USB-C cable. USB-C is the newest USB standard, increasingly adopted by portable device manufacturers. A portable hotspot with a USB-C port would be favourable to a force using other USB-C port devices, since only one cable could be used to charge multiple devices.

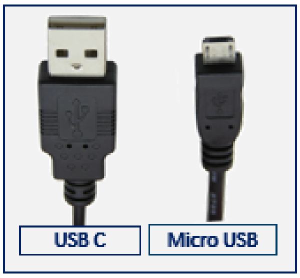

Figure 6

High quality charging cables are recommended, since they offer more protection from possible power surges and overheating, which can damage connected devices. Additionally, they reduce the risk of cable failure, which could result in officers/staff being unable to use the portable hotspot.

It is recommended that forces select a portable hotspot with a port/cable arrangement that is the same as other force devices, in order to simplify and reduce the number of chargers and charging cables required.

6.4 Security

6.4.1 Virtual Provider Network (VPN)

Virtual Private Networks (VPNs) are a highly mature technology that allows the safe and private use of unsecure, unencrypted networks. A VPN routes data coming into a user's device through servers in another location and scrambles it to make it unreadable. When connecting to any LTE or Wi-Fi service a VPN should always be used. Please see *FDM's Connection Types guideline* for more information on VPNs.

It is recommended that forces use a VPN when using a portable hotspot to provide internet access.

6.4.2 Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)

More recent portable hotspot models typically come with some security turned on by default. Usually, the manufacturer enables Wi-Fi Protected Access Pre-Shared Key (WPA-PSK). WPA-PSK is a security mechanism used to authenticate and validate users on a wireless LAN (WLAN) or Wi-Fi connection.

WPA-PSK works by configuring a WLAN passphrase or password of eight to 63 characters. Based on the password, access point (router) and connecting node credentials, a 256-character key is generated, shared and used by both devices for network traffic encryption and decryption.

There are three types of WPA-PSK: Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3). Currently, most routers and Wi-Fi connections use WPA2, because it is safe from many vulnerabilities in encryption standards. The latest upgrade for Wi-Fi Protected Access is WPA3, but it is not commonly used.

A potential problem with default portable hotspot security setups is that sometimes the default encryption strength is set to an outdated encryption standard, such as Wired Equivalent Privacy (WEP), or does not have the most secure form of encryption enabled, even though it is available as a configuration choice. Some manufacturers opt not to enable the latest and strongest security standard in an attempt to balance security with compatibility for older devices that might not support the latest encryption standards.

It is recommended that Wi-Fi Protected Access II (WPA2) is enabled as the encryption type for portable hotspots as it is current, widely used and proven to be secure.

6.4.3 Service Set Identifier (SSID) and password

A service set identifier (SSID) is the name for a Wi-Fi network. A user wanting to connect to a portable hotspot will search for an SSID, select it and enter a password (if password protected) to connect. It is recommended to change the SSID from the default to something random, avoiding dictionary words.

To improve the security of the network it is also recommended that a portable hotspot be configured to hide the SSID thereby rendering it undetectable. It is important to note that this in itself will not stop hackers intruding on a network. Hackers use precomputed hash tables for the pre-shared keys of the most common SSIDs against common pass-phrases. Hackers use “rainbow table” attacks where they try to use a precomputed hash table to crack the stored passwords.

It is recommended that forces change the wireless network password or PIN (known as the pre-shared key) to prevent others from connecting to the device without permission. Forces should follow National Cyber Security Centre (NCSC) guidance on password policies.

It is recommended that forces change the SSID, the portable hotspot's network name, from the default to something random, avoiding dictionary words. It is also recommended that the SSID is set to non-visible on portable hotspots.

It is recommended that forces change the wireless network password (known as the pre-shared key). Forces should follow National Cyber Security Centre (NCSC) guidance on password policies.

6.4.4 Port filtering

Some portable hotspots allow port filtering as a security mechanism. Port filtering is when a router monitors the destination ports of the Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or other port-based network protocol packets that pass through it, and blocks non-permitted services. Users can allow or prevent access to File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), email traffic, and other ports or services based on how the portable hotspot will be used. For example, if FTP is not going to be used it can be disabled in the port-filtering configuration page.

Port filtering comes with an administration overhead, depending on rollout procedures. Force IT departments may need to manually configure the settings on portable hotspots before roll out to end users.

It is recommended that where available, forces adopt a “deny all” policy to TCP/UDP ports and only open ports necessary for their specific use case, for example 1194 for VPN and 443 for https.

6.5 Size and weight

The size and weight of a portable hotspot is an important consideration (if the intention is for personal issue) to ensure that officers and staff are comfortable with carrying the portable hotspot in their uniform pocket. Portable hotspots come in a range of different sizes and weights. There are dual purpose portable hotspots that also function as power banks which would reduce the amount of items an officer might carry. These are covered below in section 6.6.1 Dual purpose portable hotspots.

To ensure the portable hotspot does not add additional burdensome weight to what officers and staff already need to “personal carry”, it is recommended that hotspots weigh no more than 250 grams. It is also recommended that to ensure the portable hotspot can fit comfortably into uniform pockets that it is no larger than 15cm x 10cm x 2cm.

6.6 Other features

6.6.1 Dual purpose portable hotspot

Some portable hotspots on the market have the ability to operate as a portable power bank providing remote charging to rechargeable battery powered portable devices on the go. These portable hotspots tend to have a larger battery capacity making them more expensive and often bigger and heavier.

For further information about portable power banks see FDM’s *Portable Power Banks* guideline.

Forces that are considering purchasing both portable power banks and portable hotspots are recommended to consider the purchase of dual purpose portable hotspots with portable power bank capability, as this will reduce the number of peripherals required.

6.6.2 Data storage capability

Some portable hotspots have a Micro SD slot allowing users to insert a micro SD card and plug the hotspot into a PC/laptop to use as an external USB memory stick. Portable data storage devices are not permitted by a number of forces, since they pose a data security risk.

> It is recommended that forces avoid purchasing portable hotspots with micro SD card slots, or that if these exist, they are disabled, in order to mitigate data security risks.

6.6.3 Ruggedisation

A small number of portable hotspots available are rugged or "ruggedised". This means they are designed to be hardwearing and protect against bangs and drops. They tend to have a thicker and stronger housing than non-ruggedised portable hotspots, with the aim of withstanding shock and vibration.

> While forces could benefit from having ruggedised portable hotspots, they do tend to be heavier and more expensive. Given that forces report that when selecting cheaper peripherals they are less concerned about damage it is recommended that that additional expense and weight is spared and non-ruggedised portable hotspots are selected.

6.6.4 Display

Some portable hotspots on the market currently have an LCD display that indicates information such as signal strength, number of devices connected, data usage and remaining battery capacity. Other portable hotspots have an LED indicator display that shows information such as signal strength and remaining battery however further information such as data usage would need to be obtained via the connected device.

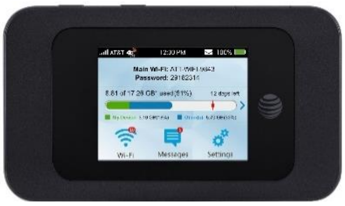

Figure 6

> While forces could benefit from having portable hotspots with LCD displays, they do tend to be more expensive. It is recommended that that additional expense is spared and portable hotspots without LCD displays are selected.

6.7 Price

Portable hotspots vary in price depending on the specification and features. Forces should consider both the upfront purchase cost of the hardware, as well as the ongoing running costs of data services. Cost is most likely to be affected by the following:

- The later the generation of cellular network, the more expensive the portable hotspot. 3G portable hotspots are the least expensive whilst 5G are the most expensive
- Ruggedised portable hotspots are more expensive
- Portable hotspots with LCD displays are more expensive
- Portable hotspots that can act as power banks are more expensive. The greater the charging capacity of the portable hotspot, the more expensive it is likely to be
- The greater the data usage, the greater the running costs

A recommended target price range for a 4G LTE portable hotspot is £60 to £80. Due to the way in which portable hotspots would be used on the frontline and coupled with the fact many forces consulted do not repair damaged low cost peripherals, portable hotspots above this price range are considered unlikely to deliver best value for money. Forces are recommended to explore bulk purchasing portable hotspots, which could reduce down the price per unit cost. Purchasing through a network provider often means users get the device itself for free, depending on the data plan contract. If a force is purchasing a dual portable hotspot and power bank, a recommended target price is up to £120.

7. How to get the best from the technology – Do's and Don'ts

Advice on how you should and should not use your portable hotspot is detailed below.

Do's	Don'ts
✓ *Do* take care when handling a portable hotspot as dropping it could damage the circuit board and/or lithium battery ✓ *Do* charge the portable hotspot with the original cable or a third party certified cable. ✓ *Do* periodically take out user-replaceable batteries to check for splits or cracks and replace if necessary.	x *Don't* expose portable hotspots to extreme temperatures as this could damage or reduce the life of the lithium battery. Since vehicles can reach high temperatures in the summer and low temperatures in the winter it is important that portable hotspots are not left inside them. x *Don't* expose portable hotspots to moisture as this could lead to water damage. x *Don't* repeatedly charge a portable hotspot to its full capacity as this will shorten the life of the lithium battery.

Table 2

DIGITAL POLICING PORTFOLIO

FRONTLINE DIGITAL MOBILITY

Digital Policing Portfolio
Portland House, Bressenden Place, Westminster, London SW1E 5RS