Protective Marking: Official

DIGITAL POLICING PORTFOLIO

Frontline Digital Mobility National Guidelines

Connection Types

March 2020

FRONTLINE DIGITAL MOBILITY

IMPORTANT NOTICE:

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	Connection Types
Version	Final
Last updated	11.03.2020
Suggested Review Date	September 2020
Owner	FDM Programme Lead
Approval by	FDM Programme Lead

CONTENTS

1. Context

Frontline officers and staff need secure connectivity in order to achieve remote access to their force systems and to be able to exchange data. Remote connectivity can be provided to frontline mobile devices, such as smartphones and tablets, either via the device's own mobile broadband capabilities (3G, 4G or 5G), or by connecting to an external Wi-Fi connection. External connection may come from a third party Wi-Fi connection (e.g. publically available Wi-Fi in a coffee shop or Wi-Fi in another agency's office), by tethering to another mobile device or in-vehicle router (that has data services), or by a portable hotspot device.

Staying connected on the frontline can also require the use of peripherals to enable mobile devices to be easier to use, such as headsets and keyboards. Peripherals can either be wired or connected wirelessly via Radio Frequency (RF) or Bluetooth.

Near Field Communication (NFC) short-range technology is becoming increasingly present on iOS, Android and Windows mobiles, and is positioned as a unique connectivity enabler. Long-range (LoRa) technology (not covered herein) has become the de facto technology for Internet of Things (IoT).

Connection types vary considerably in terms of:

- Speed of connection
- Range of applications
- Data rates
- Performance
- Security
- Reliability
- Battery drain
- Number of devices to be supported at once

This guideline will explore the main connection types used by frontline officers and staff, considering the above variances, whilst also making recommendations about security and appropriate use.

This guideline focuses on assisting forces to maximise their use of public 3G/4G (LTE) data networks prior to the delivery and adoption of the Emergency Service Network Data Services. This guideline does not cover voice services delivered over any of these networks.

All information contained within this guideline is open source, drawing on technology journals, publications and blogs.

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. Recommendations

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

Guideline ID	Recommendations	Section Reference	Guideline Theme
GL-CT-01	It is recommended that forces proceed with caution at this time when purchasing 5G enabled devices as this is currently an immature technology and there is not wide network coverage geographically.	4.1.3 5G	Availability
GL-CT-02	It is recommended that forces always use a VPN when using LTE or Wi-Fi.	3. Mobile device strategy using VPNs	Security
GL-CT-03	It is recommended that forces take up opportunities to engage with the ESN programme to understand the Public Sector LTE capabilities that will be available to them, such as prioritisation and pre-emption and the secure boundaries put in place, which mitigate security considerations.	4.1.2.1 LTE and LTE-Advanced	
GL-CT-04	It is recommended that forces disable Wi-Fi Protected Setup (WPS) on their router if the router permits it.	5.1.1 Wi-Fi	
GL-CT-05	It is recommended to 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.	5.1.2 Tethering from another mobile device or police vehicle	
GL-CT-06	It is recommended that forces change the wireless network password (known as the pre-shared key). Forces should follow Nation Cyber Security Centre (NCSC) guidance on password policies.	5.1.2 Tethering from another mobile device or police vehicle	
GL-CT-07	It is recognised that some forces do not permit the use of USB ports for anything other than the provision of power. Therefore, if USB adapters are required forces are recommended to ensure that they are permitted in line with local force security policies.	6.1 Wired peripherals	
GL-CT-08	If forces wish to purchase RF peripherals, it is recommended to purchase devices with AES encryption to protect against interception.	6.2.1 Radio frequency (RF)	
GL-CT-09	It is recommended that forces ensure their firmware and operating systems are up-to-date in order to safeguard against Bluetooth vulnerabilities.	6.2.2.1 Bluetooth security	

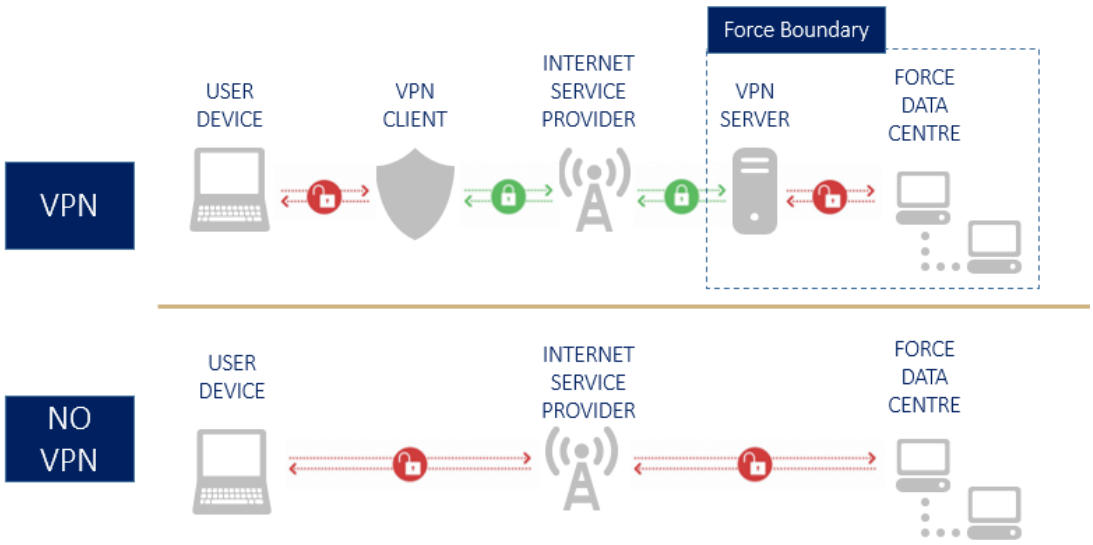
Guideline ID	Recommendations	Section Reference	Guideline Theme
GL-CT-10	It is recommended that forces ensure Bluetooth devices are configured by default as undiscoverable and remain undiscoverable except when needed for pairing. This prevents visibility to other Bluetooth devices except when discovery is required.	6.2.2.1 Bluetooth security	Security
GL-CT-11	It is recommended that forces ensure Bluetooth capabilities are disabled when they are not in use in order to minimise exposure to potential malicious activities (as well as conserve battery power). For devices that do not support disabling Bluetooth the entire device should be switched off when not in use.	6.2.2.1 Bluetooth security	
GL-CT-12	It is recommended that forces consider the use of a Mobile Device Management (MDM) solution to enforce their security policies.	6.2.2.1 Bluetooth security	
GL-CT-13	It is recommended that forces change the PIN code of Bluetooth devices, ensuring that PINs are sufficiently random, long and private (avoiding static and weak PINs such as all zeros).	6.2.2.1 Bluetooth security	
GL-CT-14	It is recommended that forces perform pairing as infrequently as possible, ideally in a secure area (non-public) to limit the chance of pairing messages being intercepted by malicious users.	6.2.2.1 Bluetooth security	
GL-CT-15	It is recommended that forces only procure and connect Bluetooth devices that are version 2.1 or higher so that Security Mode 4 can be achieved. Security Mode 4 uses Secure Simple Pairing (SSP), which protects against passive eavesdropping and man-in-the-middle (MITM) attacks.	6.2.2.1.1 Bluetooth BR/EDR/HS	
GL-CT-16	It is recommended that forces are selective when it comes to the procurement and use of Bluetooth devices that have neither a display nor input capability (e.g. headsets) as these devices connect via the Just Works association model, which provides no man-in-the-middle (MITM) protection.	6.2.2.1.1 Bluetooth BR/EDR/HS	
GL-CT-17	When considering Bluetooth devices with low energy functionality, version 4.2 or higher is recommended to provide the highest security mode.	6.2.2.1.2 Bluetooth Low Energy	

Table 1

3. Mobile device strategy using VPNs

Localised Virtual Private Networks (VPNs) are in use across UK police forces to ensure the secure and convenient sharing of data between officers and staff. VPNs are a mature technology that allows users to communicate over public, unsecure, unencrypted networks privately and safely by establishing secure encrypted connections. A VPN routes data coming into a user's device through servers in another location and scrambles it to make it unreadable. At its core, every VPN is essentially a tunnel for traffic, boring a hole through the cloud to form a secure "tube" through which traffic is safe from hackers. Most importantly, a VPN protects data, since this tunnel cannot be penetrated and transmissions cannot be viewed. The diagram below details how a VPN works.

Figure 1



The most secure VPNs hold a "no logging-policy" which states that no records are maintained of how customers of a VPN use that service.

Critically any force using a public LTE (Long-Term Evolution) data service cannot control the IP (Internet Protocol) address issued to the end user device and as such have limited options for controlling the ingress to their data centres. The introduction of a VPN allows robust ingress control to be applied to ensure that only traffic from the approved VPN solution can gain access to the data centres or cloud based services.

The use of a VPN applies to both LTE and Wi-Fi services. **Recommendations in this guideline assume that an approved VPN service is in place and that all connections are made through this service in order to protect force resources.**

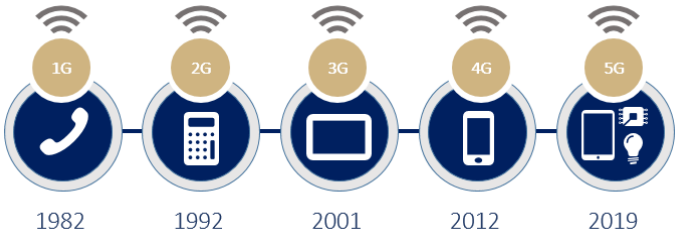
It is recommended that forces always use a VPN when using LTE or Wi-Fi.

4. Mobile data services

Remote connectivity can be provided to frontline mobile devices, such as smartphones and tablets, via cellular data services. A monthly data plan with data limits is required per device. Alternatively, group data plans may be available which provide a data allowance across multiple devices.

Wireless mobile telecommunications technology is named according to its generation. The third generation (3G) led to the adoption of the term "mobile broadband", as this is when it first became realistic to use the internet whilst being mobile. Since then, a further two generations, the fourth generation (4G) and fifth generation (5G) have been introduced. Each generation is characterised by new frequency bands, higher data rates and non-backward-compatible transmission technology.

Figure 2



4.1.1 3G

3G is the third generation of wireless mobile telecommunications technology. It was introduced in 2001 as the upgrade from earlier generations creating a more reliable and faster data transfer speed. 3G services work using a cellular based technology, with mobile devices connecting to a mast. As a mobile device physically moves around, it is passed from mast to mast, in order to maintain signal.

The speed of a 3G network depends on the strength of the mobile signal the device is receiving. The available signal is determined by the mast networks and individual capabilities of the network provider. The further away from the mast the device is, the weaker the signal. If there are a large number of users in a local network using a 3G service, the speed and signal strength will also be affected. 3G provides an information transfer rate of at least 144 Kbit/s. The typical maximum speed for downloads over a 3G network is 7.2 Mbit/s and 2 Mbit/s for uploads. There are further successors of the 3G technology - 3.5G and 3.75G, which provide faster broadband access to smartphones and mobile modems in laptops. These newer standards allow bit-rates to reach as high as 337 Mbit/s downloading and 34 Mbit/s uploading.

3G is still relevant today, even with the introduction of 4G and the emerging 5G networks, for three reasons. Firstly, it covers a much wider geographical area than the other networks. Secondly, it is a more reliable and stable network than 4G. When the 4G network connectivity is limited, users can still benefit from 3G to maintain connectivity. Lastly, it is a more efficient network; 3G tends to use less energy than 4G or 5G, conserving mobile device battery life.

4.1.2 4G

4G is the fourth generation established in 2012. It is the next evolution from 3G, offering greater speeds for data and a reduction in latency, i.e. the time taken to start loading data.

The 4G standards state that the peak speed requirements for the 4G service are 100 Mbit/s for high mobility communication, such as from trains and cars, and 1 Gbit/s for low mobility communications, such as pedestrians and stationary users.

4G candidate systems are commercially deployed as the Long Term Evolution (LTE) standard, the first iteration of 4G. This standard is a networking standard developed to provide increased speed and efficiency for mobile broadband. Although it increases the network speed, it still supports much less than 1 Gbit/s peak bit rate and is therefore not fully compliant as a 4G network. A revised version of the standard, Long Term Evolution Advanced, has since been released as a backward compatible version of LTE and promises speeds of 1 Gbit/s.

4.1.2.1 LTE and LTE-Advanced

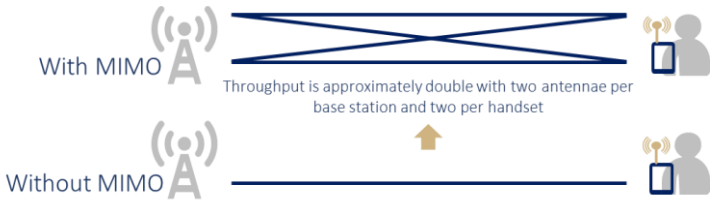
LTE is a standard for wireless communication of high-speed data for mobile phones and data terminals. It increases the capacity and speed of a connection compared to 3G as it uses a different radio interface and a core network improvement.

The evolution of mobile communication systems has not only incorporated improvements in functionality, but also strengthened security. LTE specifications have strengthened the security of connections, providing strong privacy and availability guarantees to mobile users.

Long Term Evolution Advanced (LTE-Advanced) is an enhancement of the LTE standard. It has formally been recognised as a 4G candidate as it promises the 1 Gbit/s speed. There are three technologies within the LTE-Advanced toolkit that, if used together with sufficient aggregated bandwidth, can deliver maximum peak downlink speeds of 1 Gbit/s. These technologies are: carrier aggregation, Multiple Input Multiple Output (MIMO) and modulation.

The peak download speed for a 4G LTE-Advanced connection is approximately 300 Mbit/s, whilst a standard 4G LTE download speed peaks at 150 Mbit/s. Despite this, it is likely that the real world speed of 4G LTE is around 15 Mbit/s while the 4G LTE-Advanced speed is normally between 42 Mbit/s and 90 Mbit/s, making LTE-Advanced three times faster than standard 4G LTE speeds. There are external factors that affect the speed including the proximity of a 4G mast, the device that 4G is being used on and how many users are on the network.

Figure 3



Standard data connections use one antenna and one signal at any given time, but 4G LTE-Advanced uses multiple signals and multiple antennae. It uses MIMO technology to combine multiple antennae on both the transmitter (a 4G mast) and the receiver (a smartphone). The more antennae available on both the transmitter and the receiver, the faster the potential speeds as multiple data packets are travelling in parallel.

Carrier aggregation enables the device to receive multiple 4G signals at once without them being on the same frequency. For example, it is possible to receive a 1750MHz and a 750MHz signal at the same time, which would not be possible with standard 4G-LTE technology. Up to five different signals can be combined at once. Each signal utilises up to 20MHz of bandwidth, which can be combined to create a data pipe of up to 100MHz of bandwidth.

The Emergency Services Network (ESN) programme will offer Public Services LTE (PS LTE) capabilities enabling forces to utilise prioritised and secure high-speed data and video services. During a crisis, network congestion can occur which, without network priority and pre-emption, would make it difficult for public safety personnel to communicate and maintain connectivity. ESN will provide both extended coverage and network priority and pre-emption, which will allow personnel to maintain emergency communications, coordinate with all public safety agencies and perform their jobs during critical situations.

Prioritisation and pre-emption are network capabilities. Prioritisation moves public safety personnel to the front of the "communications line", prioritising their network needs. Pre-emption goes a step further ensuring public safety personnel have access to the network first, even if services to lower priority users are denied. For example, when customers are waiting in a line, prioritisation would reshuffle the line from high to low so that the highest priority customers are always at the front of the line. Pre-emption removes the lowest prioritised customer so that the higher priority customer can begin their transaction immediately. Prioritisation is combined with pre-emption to work together to manage traffic on the network.

It is recommended that forces take up opportunities to engage with the ESN programme to understand the Public Service LTE capabilities that will be available to them, such as prioritisation and pre-emption and the secure boundaries put in place, which mitigate security considerations.

4.1.2.2 4G security considerations

There are multiple security considerations associated with using a 4G network, detailed in the table below. The network can potentially be jeopardised by many security threats due to the open nature of the architecture and standards.

Consideration	Description
Interference	A network connection can stop functioning due to a poor signal-to-noise ratio, which could be caused by man-made interference.
Scrambling Attacks	Scrambling is a form of interference which is activated for short intervals of time. An attack may be made on a particular user to disrupt service.
Signal Jamming	The LTE network is very complex, made up of many subsystems. Loss of any one subsystem can result in a loss of network service.
Location Tracking	It is possible to track a mobile device's presence in a particular cell or across multiple cells.
Denial of Service (DoS) Attacks	Denial of Service (DoS) attacks are a concern for LTE networks.
Open Nature	The open protocol architecture makes 4G wireless networks vulnerable to a range of security attacks such as Malware, Trojans and Viruses.

Table 2

4.1.3 5G

5G is the fifth generation of wireless mobile telecommunications technology. 5G speeds range from approximately 50 Mbit/s to over 2 Gbit/s and are expected to grow to 100 Gbit/s, 100 times faster than 4G. 5G began wide deployment in 2019 with every major telecommunications service provider deploying 5G antennae. The 5G spectrum is categorised into two frequency bands: mid-band and low-band. 5G low-band offers similar capacity to 4G LTE-Advanced. 5G providers have latencies between 25–35 milliseconds, which is a lower latency than 4G.

The new 5G wireless devices also have 4G LTE capability, as the new networks use 4G for initially establishing the connection with the cell, as well as in locations where 5G access is not available. 5G can support up to a million devices per square kilometre, while 4G supports only up to 100,000 devices per square kilometre.

Beyond mobile operator networks, 5G is also expected to be widely used for private networks with applications in industrial Internet of Things (IoT), enterprise networking, and critical communications. There are a number of concerns associated with 5G. These are detailed below:

- *Interference issues*
  The spectrum used by various 5G proposals will be near to that used by passive remote sensors for gathering weather data, particularly water vapour levels.
- *Surveillance concerns*
  Due to fears of potential espionage by foreign users, several countries have taken actions to restrict or eliminate the use of certain equipment in their respective 5G networks.
- *Health concerns*
  The development of the technology has elicited a range of concerns that 5G radiation could cause adverse health effects.
- *Security concerns*
  5G technology could open a new era of security threats. 5G enables the movement and access of vastly higher quantities of data and therefore broadens attack surfaces. The capacity for cyberattacks could increase proportionally.

It is recommended that forces proceed with caution when purchasing 5G enabled devices as this is currently an immature technology and there is not wide network coverage geographically.

5. Wireless network technology

Wireless technology is the alternative to traditional wired networking. Where wired networks rely on cables to connect devices together, wireless networks rely on wireless technologies. This section of the guideline will explore three examples of wireless network technologies used in policing: Wi-Fi, tethering from another mobile device or police vehicle, and portable hotspots.

5.1.1 Wi-Fi

Wi-Fi is part of a family of wireless networking technologies, based on the IEEE 802.11 family of standards, which are commonly used for local area networking and Internet access. Devices that can

use Wi-Fi technologies include desktop PCs as well as mobile devices such as smartphones and tablets. The greatest advantage of Wi-Fi is the ability to use a network without wires.

There are a number of different Wi-Fi standards, utilising different radio technologies and radio bands, and with varying maximum ranges and achievable speeds. Some versions of Wi-Fi support the use of multiple antennae, which enables greater speeds as well as reduced interference. Wi-Fi 4, 5 and the latest 6 versions are currently marketed.

Over time, the speed of Wi-Fi has increased. Wi-Fi 4 operates on 2.4GHz or 5GHz frequency bands. Wi-Fi 5 operates only on a 5GHz frequency band. The latest Wi-Fi 6 standard operates on 2.4GHz and 5GHz frequency bands but at a faster rate through more efficient data encoding, resulting in higher throughput and faster speeds. As of 2019, at close range, some versions of Wi-Fi, running on suitable hardware, can achieve speeds of over 1 Gbit/s.

A new “target wake time” (TWT) feature means that a smartphone, laptop, or other Wi-Fi-enabled device should have longer battery life. When the access point is talking to a device, for example a smartphone, it can tell the device exactly when to put its Wi-Fi radio to sleep and exactly when to wake it up to receive the next transmission. This will conserve power, as it means the Wi-Fi radio can spend more time in sleep mode.

Wi-Fi is more vulnerable than wired networks because anyone within range of a network with a wireless network interface controller can attempt access. Wi-Fi Protected Setup (WPS) is a network security standard used to protect wireless networks. There are three primary approaches to network setup within WPS: PIN entry, push button, and Near Field Communication (NFC).

- *Pin entry*
  A unique PIN (Personal Identification Number) will be required for each device to join the network. The PIN is used to make sure the intended device is added to the network being set up and helps to avoid accidental or malicious attempts to add unintended devices to the network. Pin entry is the mandatory baseline mode and everything must support it.
- *Push button*
  The user may connect multiple devices to the network and enable data encryption by pushing a button. The access point/wireless router will have a physical button, and other devices may have a physical or software-based button. The user is required to push a button, either actual or virtual, on both the access point and the wireless device. On most devices, this discovery mode turns itself off as soon as a connection is established or after a delay (typically two minutes or less), whichever comes first, thereby minimising its vulnerability. Support of this mode is mandatory for access points and optional for connecting devices.
- *Near Field Communication*
  The user is required to bring the device close to the access point to allow a near field communication between the devices. Support of this mode is optional.

WPS pin entry is affected by a major security flaw. The flaw allows a remote attacker to recover the WPS PIN in a few hours with a brute-force attack and, with the WPS PIN, the network's WPA/WPA2 pre-shared key (PSK). Users have been advised to turn off the WPS PIN feature, although this may not be possible on some router models.

It is recommended that forces disable WPS on their router if the router permits it.

To connect to a private Wi-Fi network, a user typically needs the network name (the service set identifier or SSID) and a password. The password is used to encrypt Wi-Fi packets to keep the network secure.

Public and guest Wi-Fi can be found in public places such as coffee shops and restaurants. External connections may also come from another agency's office. Public Wi-Fi does not offer the same level of security as private Wi-Fi. Despite this, it is still considered secure enough for frontline officers and staff with the use of their VPN.

It is important to note that many public and guest Wi-Fi use a captive portal; a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by. In line with national guidance, captive portals are blocked on the majority of force devices therefore forces may be unable to access public or guest Wi-Fi services that use this. Devices that have an always-on VPN will not be able to connect to Wi-Fi hotspots that use captive portals.

5.1.2 Tethering from another mobile device or police vehicle

Tethering is the sharing of one mobile device's internet connection with other connected mobile devices. This can be achieved via Wi-Fi, Bluetooth or by physical connection using a cable, for example through USB. When tethering is achieved via Wi-Fi, the feature may be branded as a "personal" or "mobile" hotspot. The internet-connected mobile device acts as a portable wireless access point and router for devices connected to it. The tethering feature is readily built into and supported by most modern mobile devices.

Mobile device tethering can allow officers and staff to access the internet from one mobile device to another (say a smartphone with mobile data to a Wi-Fi only tablet). The same can also be achieved tethering from police vehicles with in-built Wi-Fi routers. Tethering therefore presents the opportunity for forces to purchase Wi-Fi only mobile devices. 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 mobile device and /or in-vehicle tethering.

Tethering 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, 4G tethering can be used to speed up its mobile internet connection.

The main limitation of tethering is that it rapidly drains the battery of the device with mobile data. Furthermore, a device's ability to make and receive phone calls may be restricted when in tether mode.

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.
See: https://www.ncsc.gov.uk/collection/passwords [Accessed 10 Mar. 2020]

It is recommended to 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 Nation Cyber Security Centre (NCSC) guidance on password policies.

5.1.3 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 5G internet access. Multiple devices can simultaneously share the connection of a single portable hotspot that is within range of their signal. Portable hotspots are typically more reliable and faster than mobile device based hotspots, e.g. smartphone hotspots. For further information, including recommendations, relating to portable hotspots, please see *FDM's Portable Hotspots guideline*.

6. Connecting peripherals to mobile devices

Staying connected on the frontline can require the use of peripherals to enable mobile devices to be easier to use, such as headsets and keyboards. Peripherals can use wired or wireless connections.

6.1 Wired peripherals

Wired peripherals are generally cheaper than their wireless counterparts. They are compatible with all devices with a standard full size USB connection and are most often plug and play (if drivers are required they are usually easy to install). Wired peripherals connect to devices a via USB cable. Mobile devices, such as smartphones, do not have full size USB ports and therefore require an adapter, for example USB-to-Micro-USB or a USB-to-USB-C, depending on the device. Adapters add clutter to what should be a portable device. A further disadvantage of wired peripherals is the need for a connecting cable, which will be susceptible to wear and tear and could also present a ligature risk. However, wired peripherals have the advantage of providing a secure connection. For example, in the case of wired keyboards, key strokes cannot be intercepted (as they potentially could be with wireless keyboards).

It is recognised that some forces do not permit the use of USB ports for anything other than the provision of power. It would therefore be advisable to confirm if a USB adapter would be permitted in-line with local force security policies.

It is recognised that some forces do not permit the use of USB ports for anything other than the provision of power. Therefore, if USB adapters are required forces are recommended to ensure that they are permitted in-line with local force security policies.

6.2 Wireless peripherals

Wireless peripherals transmit information over the air, which creates an often-overlooked security vulnerability. There are two main types of wireless peripherals: Radio Frequency (RF) and Bluetooth. Wireless peripherals may also use infrared (IR), but these are becoming less common and so have been excluded from this guideline.

6.2.1 Radio Frequency (RF)

Radio Frequency (RF) refers to the rate of oscillation of radio waves in the range of 20 kHz to 300 GHz, as well as the alternating currents carrying the radio signals. This is the frequency band that is used for communications transmission and broadcasting. Most RF wireless devices use frequencies centred on 2.4GHz.

RF communication occurs via transmitters and receivers. The radio transmitter is inside a peripheral, for example a keyboard. A full-sized USB dongle acts as a receiver plugged into the connecting device.

RF, like any wireless transmission, can be vulnerable to interception. For example, keystrokes can be intercepted on wireless keyboards. This vulnerability can be overcome by selecting RF peripherals that have the protection of Advanced Encryption Standard (AES) security. AES is one of the most secure types of encryption available and is used by many governments and financial institutions to protect confidential data.

If forces wish to purchase RF peripherals, it is recommended to purchase devices with AES encryption to protect against interception.

6.2.2 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication, used primarily to establish wireless personal area networks (WPANs). Bluetooth does not rely on Wi-Fi, or mobile data; as long as devices are Bluetooth compatible and in close proximity to each other, they can take part in a wireless, two-way communication.

Operating in the unlicensed 2.4000 (GHz) to 2.4835 GHz frequency spectrum, Bluetooth has seen a number of revisions since the advent of version 1.0 in 1999. Versions 1.0 to 3.0 are known as Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) or “Classic Bluetooth”, with High Speed (HS) capability included in version 3.0. Bluetooth low energy was introduced in the Bluetooth 4.0 specification and updated in later versions. It is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. A Bluetooth 4.0 or later device may support both BR/EDR/HS and low energy as a “dual mode” Bluetooth device. The most recent Bluetooth specification, Bluetooth 5.2, is an improvement upon the previous Bluetooth low energy standards. It is still geared

towards low powered applications, but improves upon data rate and range. Bluetooth specifications are designed to be backward compatible - a later specification device supports higher data rates but also supports the connection mechanism and lower data rates supported by earlier specification devices.

One of the main advantages of Bluetooth is that it can connect multiple devices simultaneously. When a group of two or more Bluetooth devices are sharing information together, they form an ad-hoc, mini computer network called a piconet. One device (known as the master) acts as the overall controller of the network, while the others (known as slaves) obey its instructions.

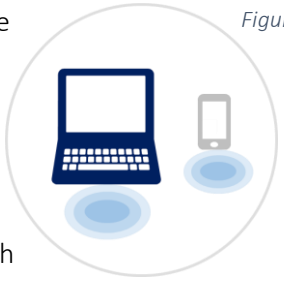


Figure 4

Other devices can join or leave an existing piconet at any time. Two or more separate piconets can also join up and share information, forming what is called a scatternet. Bluetooth uses a technique called spread-spectrum frequency hopping that makes it rare for more than one device to be transmitting on the same frequency at the same time. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. Since every Bluetooth transmitter uses spread-spectrum transmitting automatically, it is unlikely that two transmitters will be on the same frequency at the same time. This same technique minimises the risk that other devices using the same frequency band will disrupt Bluetooth devices.

6.2.2.1 Bluetooth security

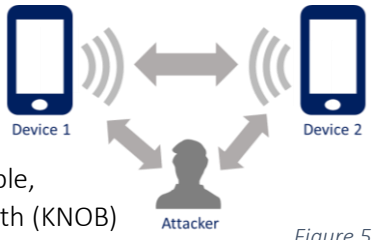


Figure 5

Devices connected via Bluetooth wireless technology can be at risk to various wireless networking threats, such as denial of service (DoS) attacks, eavesdropping and man-in-the-middle (MITM) attacks. Devices are also threatened by Bluetooth specific attacks that target known vulnerabilities in the Bluetooth architecture, for example, Bluesnarfing, Bluejacking, Bluebugging and Key Negotiation of Bluetooth (KNOB) attacks. These attacks can provide the instigators with both unauthorised access to confidential information being transferred via Bluetooth and the ability to access other systems and networks to which the devices are connected.

While numerous Bluetooth security vulnerabilities have been discovered, many have been patched through firmware and software updates.

It is recommended that forces ensure their firmware and operating system are up-to-date in order to safeguard against Bluetooth vulnerabilities.

Bluetooth devices must be “paired” with each other before they can communicate and in order to pair they must have Bluetooth enabled and be in “discoverable mode”.

It is recommended that forces ensure Bluetooth devices are configured by default as undiscoverable and remain undiscoverable except when needed for pairing. This prevents visibility to other Bluetooth devices except when discovery is required.

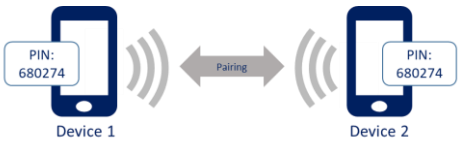
It is recommended that forces ensure Bluetooth capabilities are disabled when they are not in use in order to minimise exposure to potential malicious activities (as well as conserve battery power). For devices that do not support disabling Bluetooth the entire device should be switched off when not in use.

Forces have localised Mobile Device Management (MDM) arrangements to monitor, manage and secure officer and staff's mobile devices. Force IT departments are able to remotely configure mobile devices settings, such as Bluetooth, to align with their security policies.

It is recommended that forces consider the use of a Mobile Device Management (MDM) solution to enforce their security policies.

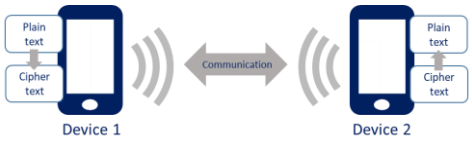
The Bluetooth standard specifies four security services:

- *Pairing*
  Creating one or more shared secret keys and the storing of these keys for use in subsequent connections in order to form a trusted device pair.



- *Authentication*
  Verifying the identity of communicating devices based on their Bluetooth address. Bluetooth does not provide native user authentication.

- *Encryption*
  Preventing information compromise caused by eavesdropping by ensuring that only authorised devices can access and view transmitted data.



- *Authorisation*
  Allowing the control of resources by ensuring that a device is authorised to use a service before permitting it to do so.

Figure 6

The pairing process often involves entering a common PIN code into each device. Bluetooth devices are often set up to use default PIN codes such as "0000" or "1234". The use of default PIN codes leaves the devices vulnerable to malicious threats.

It is recommended that forces perform pairing as infrequently as possible, ideally in a secure area (non-public) to limit the chance of pairing messages being intercepted by malicious users.

It is recommended that forces change the PIN code of Bluetooth devices, ensuring that PINs are sufficiently random, long and private (avoiding static and weak PINs such as all zeros).

6.2.2.1.1 Bluetooth BR/EDR/HS

Bluetooth BR/EDR/HS defines authentication and encryption security procedures that can be enforced during different stages of communication setup between peer devices. Link-level enforced refers to authentication and encryption set-up procedures which occur before the Bluetooth physical link is completely established. Service-level enforced refers to authentication and encryption setup procedures which occur after the Bluetooth physical link has already been fully established.

Every Bluetooth device must operate in one of the four security modes defined by the Bluetooth BD/EDR/HS specifications. The different modes determine when a Bluetooth device initiates security protocols and ultimately the strength of the security.

- *Security Mode 1*
  Security Mode 1 is considered non-secure because authentication and encryption protocols are not supported.
- *Security Mode 2*
  Security Mode 2 is a service level-enforced security mode. All 2.0 and earlier devices can support Security Mode 2, but 2.1 and later devices can only support it for backward compatibility with 2.0 or earlier devices.
- *Security Mode 3*
  Security Mode 3 is a link level-enforced security mode. All 2.0 and earlier devices can support Security Mode 3, but 2.1 and later devices can only support it for backward compatibility purposes.
- *Security Mode 4*
  Security Mode 4 is a service-level enforced security mode which uses Secure Simple Pairing (SSP). Security Mode 4 is mandatory for communication between 2.1 and later devices.

SSP simplifies the pairing process by providing a number of association models that are flexible in terms of device input/output capability. SSP also improves security by providing protection against passive eavesdropping and man-in-the-middle (MITM) attacks during pairing.

It is recommended that forces only procure and connect Bluetooth devices that are version 2.1 or higher so that Security Mode 4 can be achieved. Security Mode 4 uses Secure Simple Pairing (SSP) which protects against passive eavesdropping and man-in-the-middle (MITM) attacks.

The four association models offered in SSP are as follows:

- *Numeric Comparison*
  Designed for when both Bluetooth devices are capable of displaying a six-digit number and allowing a user to enter a “yes” or “no” response. During pairing, a user is shown a six-digit number on each display and provides a “yes” response on each device if the numbers match. If the user responds “no” then pairing fails. The displayed number is not used as input for link key generation and therefore cannot be used by an eavesdropper to determine the resulting link or encryption key.

- *Passkey Entry*
  Designed for when one Bluetooth device has input capability (e.g. keyboard), while the other device has a display but no input capability. The device with display only shows a six-digit number that the user then enters on the device with input capability. As with the Numeric Comparison model, the six-digit number used in this transaction is not incorporated into link key generation.

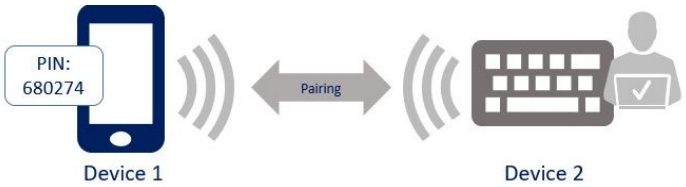


Figure 7

- *Just Works*
  Designed for the situation where at least one of the pairing devices has neither a display nor input capability (e.g. headset). The user is required to accept a connection without verifying the calculated value on both devices, so Just Works provides no MITM protection.
- *Out of Band (OOB)*
  Designed for devices that support a common additional wireless (e.g. Near Field Communication (NFC)) or wired technology. In the case of NFC, the OOB model allows devices to pair by simply "tapping" one device against the other, followed by the user accepting the pairing via a single button push.

It is recommended that forces are selective when it comes to the procurement and use of Bluetooth devices that have neither a display nor input capability (e.g. headsets) as these devices connect via the Just Works association model which provides no man-in-the-middle (MITM) protection.

6.2.2.1.2 Bluetooth Low Energy

Bluetooth Low Energy security is different from Bluetooth BR/EDR/HS, although with the Bluetooth 4.1 and 4.2 releases, the differences have been minimised.

Low Energy security modes are similar to BR/EDR service-level security modes (i.e. Security Modes 2 and 4) in that each service can have its own security requirements. However, Bluetooth Low Energy also specifies that each service request can have its own security requirements as well.

There are two low energy security modes: Low Energy Security Mode 1 and Low Energy Security Mode 2. Security Mode 1 is the most secure mode because it requires authenticated Low Energy Secure Connections Pairing. Low Energy 4.2 added a Secure Connections Only Mode, which requires that only Low Energy Security Mode 1 may be used for all services.

When considering Bluetooth devices with low energy functionality version 4.2 or higher is recommended to provide the highest security mode.

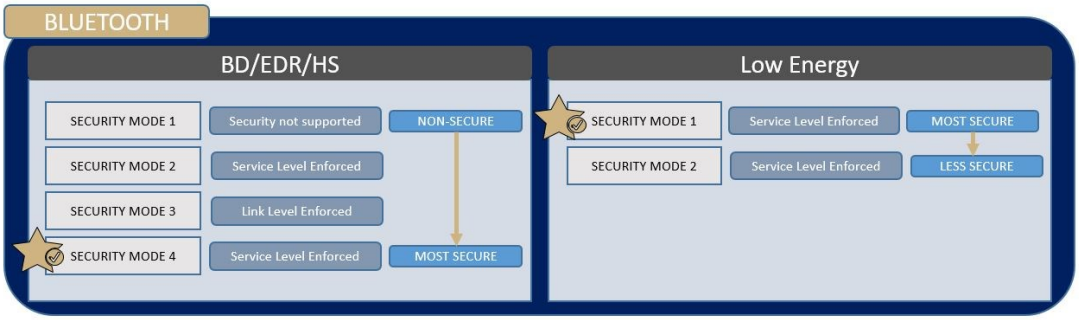

BLUETOOTH
BD/EDR/HS
SECURITY MODE 1
Security not supported
NON-SECURE
SECURITY MODE 2
Service Level Enforced
SECURITY MODE 3
Link Level Enforced
SECURITY MODE 4
Service Level Enforced
MOST SECURE
Low Energy
SECURITY MODE 1
Service Level Enforced
MOST SECURE
SECURITY MODE 2
Service Level Enforced
LESS SECURE

Figure 8

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