

# CYBER GUIDELINE DOCUMENT

## NCSP Bluetooth Guidance Document

### ABSTRACT:

This guideline provides audiences with background information concerning Bluetooth technology and guidance on how it can be suitably and securely deployed within the Law Enforcement environment.

It's purpose is to provide relevant information, enabling users of Bluetooth technology to achieve operational capability whilst minimising the risks of data security compromise.

<b>ISSUED</b>	March 2025
<b>PLANNED REVIEW DATE</b>	February 2026
<b>DISTRIBUTION</b>	Community Security Policy Framework Members
<b>POLICY VALIDITY STATEMENT</b> This guideline is due for review on the date shown above. After this date, this document may become invalid.  Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.	

# CONTENTS

Community Security Policy Commitment.....	3
Introduction .....	3
Owner .....	3
Purpose .....	4
Audience .....	4
Scope.....	5
What is Bluetooth? .....	5
How secure is Bluetooth? .....	7
Common Bluetooth Attacks .....	7
Possible Routes to Compromise .....	8
Bluetooth Best Practice .....	9
Requirements .....	9
Communication approach .....	15
Review Cycle .....	16
Document Compliance Requirements.....	16
Equality Impact Assessment .....	16
Document Information .....	17
Document Location.....	17
Revision History .....	17
Approvals .....	17
Document References .....	18

## **Community Security Policy Commitment**

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline, in conjunction with the National Policing Community Security Policy Framework and associated documents, sets out National Policing requirements.

## **Introduction**

Bluetooth technology is an integral part of our lives, and a highly adaptable means to aid data transit and delivery. More and more people have access to, and use of, technology assets equipped with Bluetooth. These include (but not limited to) laptops, mobile devices, printers, keyboards, and headsets.

Today's devices tend to have fewer USB ports and, instead, rely on wireless communication technology to provide connectivity to peripherals such as a wireless mouse, keyboard, headset, or vehicular-based wireless hands-free kits.

It is important, therefore, that users are educated on the security risks posed through connecting peripheral devices and that, at an organisational level, technical controls are applied to restrict or disable access from these devices if not required.

This guidance document aims to provide important information to assist law enforcement agencies to make informed decisions about using Bluetooth technology in their operations. By taking a cautious approach and implementing appropriate security measures, organisations can ensure a secure and safe use of Bluetooth enabled devices.

## **Owner**

National Chief Information Security Officer (NCISO).

## **Purpose**

The purpose of this guidance document is to provide policing and law enforcement organisations with relevant information regarding risks associated with deploying Bluetooth technology within the workplace, and to enhance the risk-based decisions required in the use of such technology.

The purpose of this guidance is to:

- Provide relevant information regarding Bluetooth technology
- Empower organisations to conduct suitable risk/benefit analysis prior to deployment/use of Bluetooth technology
- Encourage organisations to take a risk-based approach to their selection, deployment and use of Bluetooth technology
- Provide relevant information that allows organisations to manage any risk associated with the deployment and use of Bluetooth technology
- Provide guidance of best practice on selecting, deploying, and managing Bluetooth enabled devices, based on industry standards and best practices.

## **Audience**

All UK Home Office and non-Home Office police forces, including other law enforcement agencies.

This guidance is aimed at:

- Information Security Officers (ISOs), information security practitioners and any roles who plan, undertake and review penetration tests or ITHCs.
- Member Senior Information Risk Owners (SIROs), and Information Asset Owners (IAOs.)
- Third parties who act as service providers or suppliers to members.
- Auditors providing assurance services to members.

## **Scope**

This guidance applies to any member of the Policing Community of Trust. It is also applicable to third parties to the policing community.

## **When**

This guidance should be referred to as part of any decision-making in relation to the selection, procurement, deployment and use of any Bluetooth technology within the law enforcement arena.

## **Where**

The guidance should be referred to for application of Bluetooth technology in any scenario, and it is not geographically restricted.

## **What**

The guidance applies to the use of any Bluetooth technology deployed to send/receive, store, amplify or otherwise process any policing data / data consumed as part of policing and law enforcement business functions. This includes mobile / smart phones, tablets, body worn technology, cameras, recording equipment, navigation aids, in-vehicle technology, smart speakers, device remote controls, drones and any device capable of connecting using Bluetooth.

## **What is Bluetooth?**

Bluetooth is technology that uses a band of radio frequencies to share data over a short distance. The Bluetooth frequency band is available worldwide. The current standard is Bluetooth Core 6.0, released by the Bluetooth Special Interest Group in early September 2024.

Bluetooth Core 6.0 has introduced new features, not least of which is improved capabilities in device range detection, through Bluetooth Channel Sounding, which allows devices to accurately measure the physical distance between each other via round-trip time (RTT) and phase-based ranging (PBR) for accurate distance measurement. This update should provide greater accuracy in devices determining their relative positions to each other, and provide a greater degree of confidence that only the intended device/s is being communicated with and connected.

In terms of the physical range for transmission of data between devices, Bluetooth 5.0 had a reported typical transmission distance of 40 metres. However, whilst the signal range of this standard is greater than that of previous standards (there are reports of transmission capabilities >200m (Wankhede, 2024)), it should still be noted that the further devices are from each other, the greater the impact of signal to noise ratio. The lower the ratio, the greater the likelihood of communication loss. Similarly, to achieve greater range, Bluetooth devices must sacrifice data transmission speeds. At time of writing, no detail can yet be found regarding the transmission capabilities (range) of Bluetooth Core 6.0.

Whilst Bluetooth can provide easy ways to pair devices for data sharing, it can enable attackers

unauthenticated access, which can lead to data loss or maliciously modifying devices remotely.

Further reading on Bluetooth Core 6.0 can be found at [Bluetooth® Core 6.0 Technical Overview | Bluetooth® Technology Website](#) and general information via the Bluetooth Technology website <sup>1</sup>

---

<sup>1</sup> See <http://www.bluetooth.com> – external site

## **How secure is Bluetooth?**

Due to the short range of transmission, Bluetooth as an attack vector can be less likely, as threat actors are required to be within close proximity to their target.

Whilst the Bluetooth standard has device authentication, it does not include user authentication. This means that when communicating over Bluetooth you should verify the person handling the Bluetooth enabled device.

Bluetooth data transmissions are encrypted. The 5.0 and later standards use Advanced Encryption Standard (AES), which is the current industry standard. However, many devices still use older standards (Bluetooth 4.0 and earlier) with decreasing levels of inbuilt security the lower down the standard you go. It is important that organisations understand what devices are being deployed (asset tracking), the Bluetooth version (standard) for each device, the application for which the device is being deployed (e.g. in-car hands-free) and the type of data being processed.

Whilst devices may claim full compliance with the Bluetooth standards, hardware or software may be present that increase risks. Official devices must be suitably configured, hardened and managed in line with Force / organisational security policies. Devices are typically backwards compatible which increases risk when using legacy equipment. Configurations should enforce the later versions (v5.0 or later.)

## **Common Bluetooth Attacks**

Basic tools can be used to gather information about devices without any interaction by potential victims. These tools are used to undertake reconnaissance or collect geo-information about premises, people, or operations.

- **Bluebugging:** is a type of Bluetooth attack where an attacker gains unauthorised access to your device and takes control of it remotely. This can allow the attacker to make calls, send messages or access sensitive data on the device without the owner's knowledge.
- **BlueJacking** - When a device leaves its Bluetooth enabled, it can be discovered by threat actors looking for open connections and can receive unwanted messages.
- **BlueSnarfing** - When a device leaves its Bluetooth enabled, it can receive unsolicited pairing where a threat actor can then retrieve data from the device.
- **Denial of service** – As with any wireless technology, in the presence of strong signals the reliability of connections can be disrupted or interrupted.
- **Car Whisperer** - allows an attacker to send to or receive audio from vehicle Bluetooth equipment. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop.)

## Possible Routes to Compromise

Bluetooth is not a typical attack vector. The threat actor must be in close proximity, and the reward of connecting to a phone is fairly low, compared to other police infrastructure. However, particular care and consideration should be given in the deployment of resources to sensitive locations, including:

- Private addresses of principals/police officers & staff/military personnel/gov't agents and their employees
- Safe havens, e.g. women's refuges
- Any strategic or tactical location relating to covert, CT or OCG operations.

Due to Bluetooth being used with location finding services, any **deployments to sensitive locations** must be accompanied by messaging/protocols to **ensure Bluetooth is switched off** or hidden.

- For higher risk / sensitive areas RF pouches or RF lockers should be used to temporarily store devices

Typical attacks can be conducted with minimal tools and expertise which can lead to data leaks, gathering intelligence about people, devices and locations and unsolicited harmful software being delivered, affecting device integrity. Examples include:

- Identifying people operating out of discrete / covert locations,
- mapping movements of personnel,
- capturing of conversations or keystrokes (including passwords) and
- remotely installing eavesdropping software on mobile phones.

It is also worthy of note that data transfers over Bluetooth may not be visible to Data Loss Prevention / information management tools, thereby providing a route for unauthorised data sharing.

## **Bluetooth Best Practice**

Whilst Bluetooth can provide a neat solution for connecting multiple devices, there are security risks present in the use of this technology. The points below should be considered as best practice and as part of a local risk assessment when deploying Bluetooth based solutions.

## **Requirements**

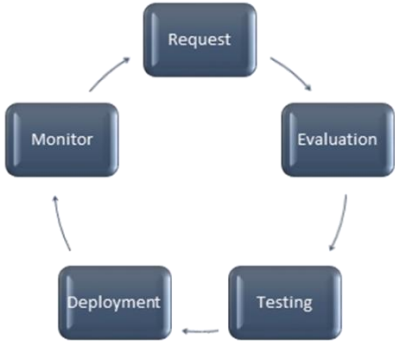
(Align the requirements -actions to take, to specific controls and control objectives. Include suggestions for measurements to help evidence / monitor compliance. Example given below.)

Reference	Minimum requirement	Control reference	Compliance Metric
<b>Legitimacy of Use</b>			
CSP-BLU-001	Is Bluetooth required? There are various methods to share data, is Bluetooth the best method/ is it required? If not, then devices should disable Bluetooth or consider low power modes where available.		<ul style="list-style-type: none"> <li>Business case supporting specifics of Bluetooth deployment.</li> </ul>
CSP-BLU-002	The use of Bluetooth for police issued devices must always be considered in the context of properly configured, organisation managed assets. Poorly configured or unmanaged devices will represent the most vulnerable targets to attacks or compromise.	ID.RA-01 PR.PS-01	<ul style="list-style-type: none"> <li>Bluetooth devices captured / included within organisational asset tracker.</li> </ul>
CSP-BLU-003	Develop an asset tracker for devices using Bluetooth & review every 6-12 months. Refer to <i>NCSP Physical Asset Management Standard</i> for further information.	ID.AM-1	<ul style="list-style-type: none"> <li>Evidence that Bluetooth devices are included within asset tracker and have appropriate review dates associated with each device.</li> </ul>
<b>Configuration controls</b>			

## NCSP Bluetooth Guidance Document

CSP-BLU-004	<p>Technical policies should be put in place to prevent or control, as well as monitor, data transfer via Bluetooth on corporate devices. This will help to manage risks around Data Loss Prevention. This should include limiting communication to v5.0 or later only.</p>	DE.CM-01	<ul style="list-style-type: none"> <li>Evidence of technical policies governing Bluetooth usage.</li> </ul>
CSP-BLU-005	<p>The NEP Blueprint Volume 5 on Mobility describes device configuration MEM Intune configuration policies which can help protect devices, by controlling a multitude of settings and features. For example:</p> <ul style="list-style-type: none"> <li>restrict use of hardware features on the device such as the camera or Bluetooth and</li> <li>configuring compliant and noncompliant apps. Administrators can be alerted if a non-compliant app is installed.</li> </ul> <p>For further information force administrators should visit 'Apply features and settings on your devices using device profiles in Microsoft Intune'.</p>	PR.PS-01	<ul style="list-style-type: none"> <li>Adherence with NEP blueprints, supported by SyAP compliance metrics.</li> </ul>
CSP-BLU-006	<p>Control the installation of applications (apps) on devices where Bluetooth is enabled. Some applications have been known to have excessive permissions which allows access to Bluetooth channels or data which might be used maliciously.</p> <p>Refer to the <i>NCSP guidance on Mobile Applications</i> for more information and utilise the following lifecycle in all cases:</p>	ID.RA-09	<ul style="list-style-type: none"> <li>Evidence of relevant app management process.</li> <li>Evidence of app lifecycle documented in organisational technical processes</li> </ul>

## NCSB Bluetooth Guidance Document

			
CSP-BLU-007	<p>Keep devices updated - Android and Apple will often include Bluetooth vulnerability updates within their wider operating system updates. Keep devices updated to mitigate the time the device is vulnerable.</p> <p>Minimise the permissions that applications (apps) on devices have to access Bluetooth.</p>	ID.AM-08	<ul style="list-style-type: none"> <li>Evidence of compliance from output of regular security testing.</li> </ul>
CSP-BLU-008	<p>Where possible, ensure you are using the latest Bluetooth standard (v5.0 or later). This will ensure you are using the most secure iteration (improved encryption) and fastest transmission of data. This can be achieved by purchasing devices through a trusted supply chain and keeping devices up-to-date and patched (see below) and in line with technical policies.</p>	ID.RA-09 PR.PS-03	<ul style="list-style-type: none"> <li>Asset tracker</li> </ul>
<b>Pairing</b>			
CSP-BLU-009	<p>Only pair police-issued devices. Personal devices should never be paired with police assets (this should include wireless home printers, wearable technology such as watches, fitness trackers, headphones etc.)</p>	PR.PS-01	<ul style="list-style-type: none"> <li>Asset tracker</li> <li>Security Testing</li> <li>Regular device 'housekeeping' (re-pairing only with known and trusted policing assets /</li> </ul>
CSP-BLU-010	<p>Police-issued devices should never be paired to smart devices / Internet of</p>	PR.PS-01	

## NCSP Bluetooth Guidance Document

	Things (IoT) devices e.g. Google, Alexa, Siri or wireless cameras (BWV devices being an obvious exception to this). Further guidance may be found within forthcoming <b>NCSP guidance documents 'Conferencing Tools Guidance' and 'IoT Guidance'</b> .		deletion of other connected devices)
CSP-BLU-011	Unpair devices as needed – When Bluetooth devices are not required, or are no longer in operation, they should be unpaired from any other police tech/devices. This must always include unpairing devices from hire cars / non-police vehicles.  Always remove previously paired devices from the 'Previously connected device' list. Efforts should also be made to remove personal data from paired equipment such as sat-navs and entertainment systems.	ID.AM-08	
CSP-BLU-012	Verify who you are pairing with - Without technical user authentication, it is good practice to physically verify the user handling the device you are communicating with.	PR.AA-01 PR.AA-03	
CSP-BLU-013	Don't pair devices in public – With the limited operating range of Bluetooth devices, pairing requests should be made away from public areas wherever possible, especially transport hubs or crowded places.	PR.AA-06 PR.IR-01 PR.IR-02	
CSP-BLU-014	Ensure that default pairing codes are changed before issue where practicable.  Regular pairing code changes: To complete	PR.PS-01	

## NCSB Bluetooth Guidance Document

	a Bluetooth connection, devices will often request a user to input a 4-digit code (or 6-digit across higher BT standards and equipped devices). The default pairing codes are widely available and therefore make devices vulnerable to unwanted connections.		
<b>Device specific</b>			
CSP-BLU-15	<p>Seized devices that have Bluetooth capability should be assumed to have Bluetooth switched on.</p> <ul style="list-style-type: none"> <li>Consider use of RF pouches or Faraday bags.</li> <li>Seek advice from Force Technical Support Units (TSU's) or their equivalents.</li> </ul> <p>Seek technical advice on safe storage prior to Bluetooth-equipped devices being taken to police premises.</p>		<ul style="list-style-type: none"> <li>Evidence of documented process for the management and storage of seized Bluetooth-capable devices.</li> </ul>
CSP-BLU-16	Change default settings in devices to ensure that controls are in place through choice.	PR.PS-01	<ul style="list-style-type: none"> <li>Documented process for all newly acquired devices to remove defaults.</li> </ul>
CSP-BLU-017	Correct configuration - Some devices can be configured to only allow simple Bluetooth connections such as from mouse and keyboards, while blocking connections from complex devices that are more likely to cause harm.	PR.PS-01	<ul style="list-style-type: none"> <li>Evidence that device management standards and processes are followed (e.g. alignment with Blueprints and SyAP outputs)</li> </ul>
CSP-BLU-018	<p>Avoid choosing device names that might disclose the owner, function, business or device type. Avoid naming Bluetooth devices in a way that identifies them as police assets. Example:</p> <ul style="list-style-type: none"> <li>Covert_Car</li> </ul>	PR.IR-01	

## NCSP Bluetooth Guidance Document

	<ul style="list-style-type: none"><li>Control_Room_Headset_1</li><li>Custody_Printer</li></ul>		
Geo-location			
CSP-BLU-019	<p>Avoid use of Bluetooth at or near sensitive locations.</p> <ul style="list-style-type: none"><li>Implement Zones for higher risk / sensitive areas, to enforce restrictions on the use of devices which may be capable of using Bluetooth.</li></ul> <p>RF pouches or RF lockers should be used to temporarily store devices.</p>	PR.IR-01 PR.IR-02 PR.AA-06	<ul style="list-style-type: none"><li>Documented policies and processes for deployments to sensitive locations and sensitive operations.</li></ul>
CSP-BLU-020	<p>Avoid use of Bluetooth during covert, CT or OCG-related operations.</p>		
User education & awareness			
CSP-BLU-021	<p>Reinforce safe use of Bluetooth behaviours, through engagement with users e.g. via End User Device Agreements, Security Operating Procedures (SyOPs), regular reminders to staff, bulletin updates etc.</p> <p>Where the capability exists, conduct Bluetooth scanning to highlight devices that are enabled. This may be included in IT health-checks – see <b>NCSP Security Testing Standard</b>.</p>	PR.AT-01	<ul style="list-style-type: none"><li>Evidence of learning &amp; development resources available to all staff (and contractors, where appropriate) that covers security awareness training.</li><li>Evidence that EUD agreements exist and are regularly updated / annual refresh</li><li>Evidence that SyOPs exist and are regularly updated / refreshed and user acceptance regularly refreshed</li></ul>

## **Communication approach**

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this guideline can also form part of regular cyber management reporting.

## **Review Cycle**

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the guideline continues to meet the objectives and strategies of the police service.

## **Document Compliance Requirements**

(Adapt according to Force or PDS Policy needs.)

## **Equality Impact Assessment**

(Adapt according to Force or PDS Policy needs.)

## Document Information

### Document Location

<https://knowledgehub.group/web/national-standards/policing-standards>

### Revision History

Version	Author	Description	Date
1.7 (approved as 2.0)	PDS Cyber	Annual review and transposition into updated template.  Updated to reflect technology market changes.	January 2025

### Approvals

Version	Name	Role	Date
1.7 (approved as 2.0)	NCPSWG	National Cyber Policy & Standards Working Group	05/03/25

## Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021
<a href="https://www.ncsc.gov.uk/10-steps-to-cyber-security">10 Steps to Cyber Security - NCSC.GOV.UK</a>	Web Page	05/2021
Bluetooth Technology website <a href="https://www.bluetooth.com/">https://www.bluetooth.com/</a>	Web Page	
Android Authority website <a href="https://www.androidauthority.com/bluetooth-1-0-to-6-0-explained-how-do-bluetooth-versions-differ-1234567890/">Bluetooth 1.0 to 6.0 explained: How do Bluetooth versions differ?</a>	Web Page	October 2024
Secure Development Standard	NCSP document	V1.0
Physical Asset Management Standard	NCSP document	V1.0
Security Testing Standard	NCSP document	V1.0
Mobile Application Guideline	NCSP document	
Internet of Things Guideline	Forthcoming NCSP document	
Conferencing Tools Guideline	Forthcoming NCSP document	