Who else is in your car with you?

Vehicle security

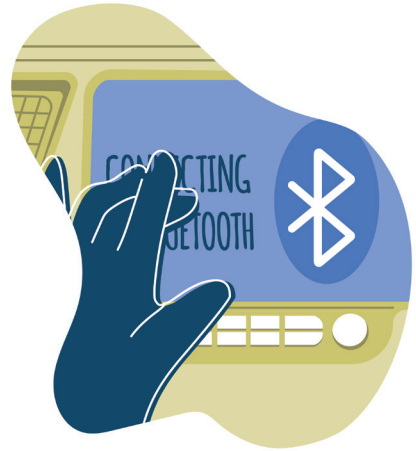
A guide for all employees

CPNI
Centre for the Protection of National Infrastructure

Introduction

Vehicle technology is evolving at an ever-increasing pace. Many vehicles now:

- fully connect to the internet, with traffic and map updates streamed to the vehicle infotainment unit;
- have touchscreen interfaces for the driver to access functionality;
- provide hands-free access for mobile phones;
- constantly update the manufacturer with their status and location;
- contain internal and external cameras for driver safety; and
- provide increasing levels of driver assistance and autonomous functionality.



While all of these things improve the driver experience and, in some cases, driver and road user safety, every new piece of technology installed has the potential to alter the risk that that vehicle poses to our official activities.

Whether you're driving a vehicle from our own internal fleet, a vehicle that the office has leased, or a rental vehicle within the UK or overseas, it's up to you to understand what risks the vehicle and its technology might pose to your activities. This guidance has been developed to help you make better and more informed choices as to how you go about any work that requires you to use or interface with a vehicle.

For further details, please refer to PALMIST within the office.

Understanding and assessing the risks

Risks associated with vehicle usage will vary depending on a variety of factors – by reflecting quickly on how and why you're using your vehicle, you could lower the level of the overall risks that you face.

There are a number of factors that should be considered, outlined in the next few pages.

How sensitive is the vehicle or your journey?

You need to consider the sensitivities of the vehicle you're using or the journey that you're undertaking. **Key considerations include:**

- whether the vehicle is always stored in a secure location;
- whether there is likely to be an interest from hostile actors in the bulk data that sits behind any fleet management system;
- whether you're also carrying an active mobile device (if you are, please refer to current security advice on mobile devices);
- what the start/end points of the journey you are undertaking are;
- whether the route itself is of interest to a hostile actor; and
- what technology is on the vehicle that might contravene security practice at the site you're visiting – for example, dashcams or on-board reversing cameras could pose a risk at sensitive sites that ban the use of cameras.

If either of the first two bullet points applies to you, there's increased risk to using that vehicle.

Many of these things have probably already been considered as part of your normal approach to work. However, we sometimes forget to look at the technology that a vehicle actually contains. Understanding the impact and risk that vehicle technology will have is important, as it may change the overall way you approach the situation.

How sensitive are the occupants?

Key considerations include:

- who will be in the vehicle; and
- why will each individual be in the vehicle.

If the potential occupants are of interest to hostile actors, the interest the hostile actor is likely to show in the occupants could alter the risk to both yourself and the vehicle.

In some cases, who the other occupants are might influence your choice of vehicle – whether that is choosing an older vehicle that has less connectivity or opting for a CAV (Civilian Armoured Vehicle) that might require a different approach to your journey planning.

What are you using the vehicle for?

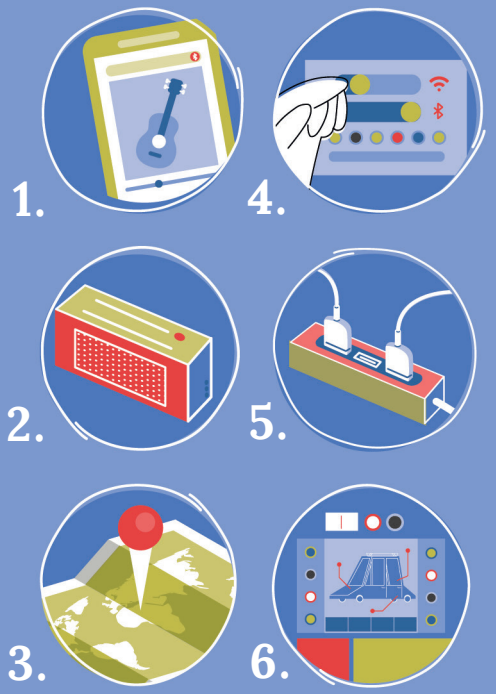
Key considerations include:

- whether you'll be having conversations of a sensitive nature within the vehicle; and
- if the vehicle will be used to temporarily store sensitive items.

Different vehicle technologies pose different risks and will therefore impact on which vehicles are suitable for certain situations.

Six ways to secure your vehicle

Understanding vehicle risks is important, but there are certain things that you should always think about when using vehicles as part of your work. Follow this guidance to help you use your vehicle in the most secure way possible.



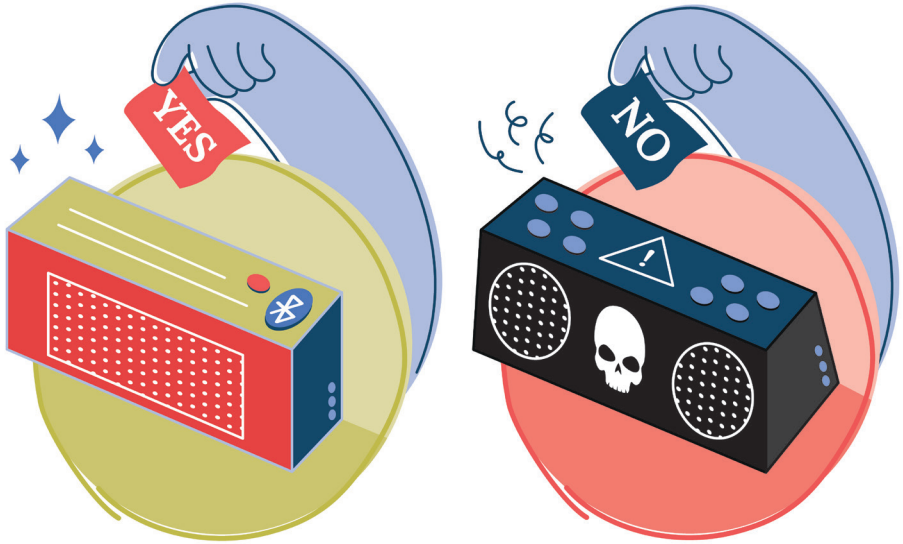
1.

Don't connect any device – work phone, personal phone or tablet – to your vehicle's Bluetooth system. You don't know where that data will end up.

The default action of a device that connects to a vehicle system is to synchronise data between the device and the vehicle. At a minimum, that means that the whole phone book on the device is copied to the vehicle, even when you deny permission. However, messages, emails, calendar, notes and images may also be included in this synchronisation process. All data is retained on the vehicle system even after you have disconnected the device – deleting the data from the vehicle system might not actually remove it, but only hide it from casual access.

2.

Do use a third-party Bluetooth hands-free kit to avoid a data breach, **but** make sure it is from a reputable dealer.



Using a third-party Bluetooth hands-free kit allows you to retain hands-free phone usage and comply with the law relating to phone use while driving. It also allows you to protect the information that you might have on your device - your data remains with you, not your vehicle.

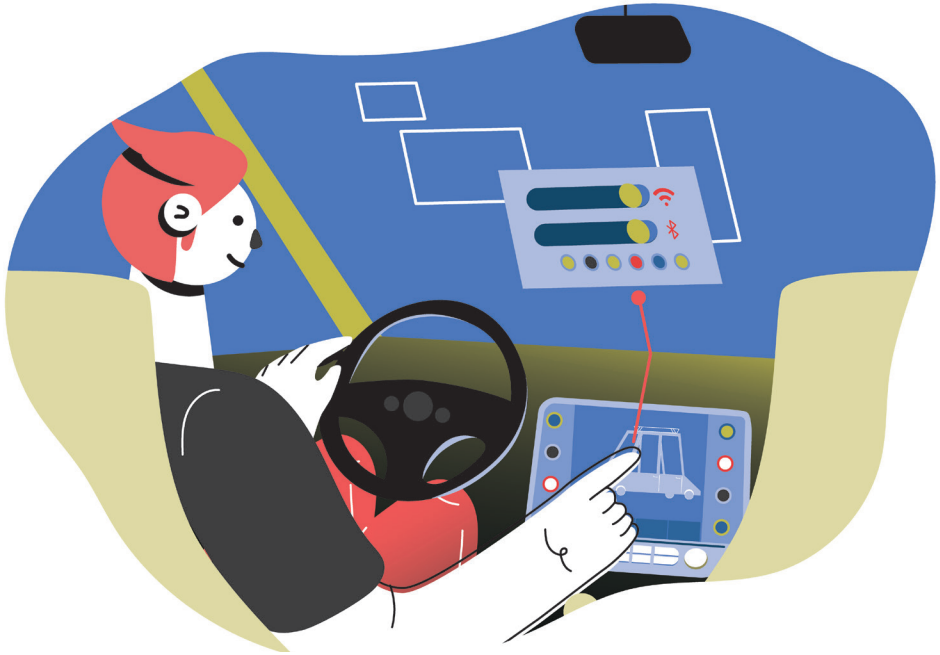
3.

Don't enter information into your vehicle's on-board SatNav system – these addresses can't be deleted. **Do** use an aftermarket SatNav for your journey.

Entering information into the on-board SatNav system leaves a trail that could be of interest to a hostile actor. As it's extremely difficult to permanently remove information from any on-board system, it's best not to enter it at all. By using a third-party SatNav system, your trip data remains with you, not your vehicle.

4.

Don't enable on-board WiFi or Bluetooth. **Do** check to ensure that they are switched off at all times.



Vehicle WiFi and Bluetooth should be disabled and not used – they allow tracking and identification of the vehicle, and provide a way for a hostile actor to access on-board systems. By disabling these technologies, you're also removing the temptation to use them to connect your own digital devices to the vehicle. Connecting an internet-enabled device to the vehicle turns a non-connected vehicle into a connected vehicle, increasing the risk to you, other occupants of the vehicle and your work.

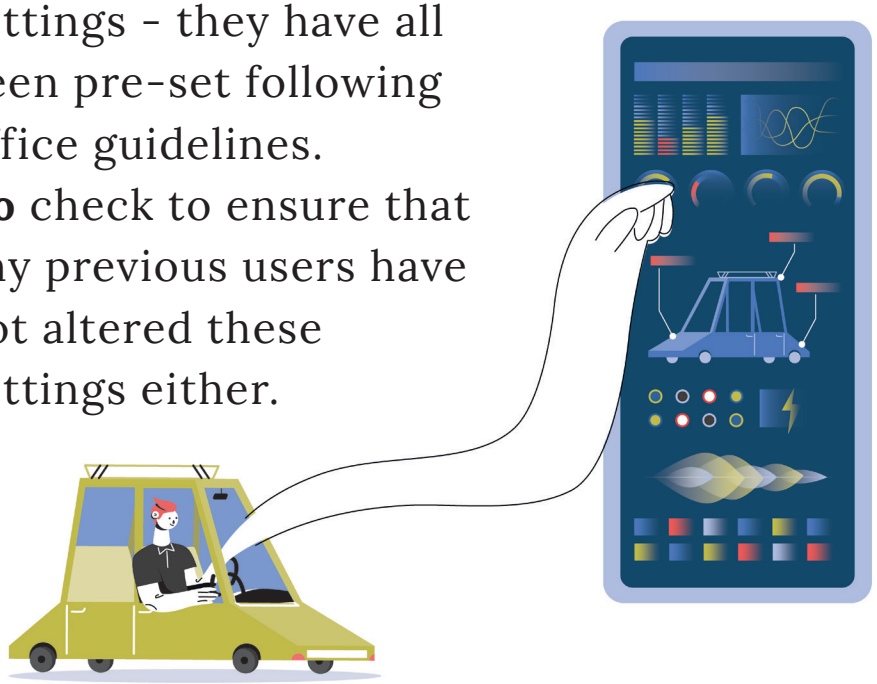
5.

Don't plug any devices into the USB ports in the vehicle. Vehicle USB ports are not just power points - they also carry data. **Do** use an adapter for your USB that plugs into the power socket or cigarette lighter.

When any device is plugged into an on-board USB port, a data connection is made and the vehicle will attempt to access and download data from your device. Always use a charging unit that you're sure only provides power and nothing else. USB chargers that plug into the vehicle cigarette lighter are common and reliable, although you should always make sure you purchase the charger from a reputable dealer.

6.

If you're using an office vehicle, **don't** change any of the vehicle's electronic settings - they have all been pre-set following office guidelines.
Do check to ensure that any previous users have not altered these settings either.



All office vehicles will have been subject to an electronic systems risk assessment by trained and qualified staff, and proportionate mitigations implemented. Therefore no electronic system should be changed or interfered with. Re-enabling or activating systems that have been disabled may be a breach of operating procedure and could result in disciplinary action.

It's also good practice to check the vehicle prior to use to make sure that a previous user has not altered any of these settings. If you're in any doubt, raise this with the technical staff – you're responsible for the security of how you do your work. If someone has re-enabled a service on the vehicle, it should be disabled – as it's also your security they are risking.

CPNI
Centre for the Protection of National Infrastructure