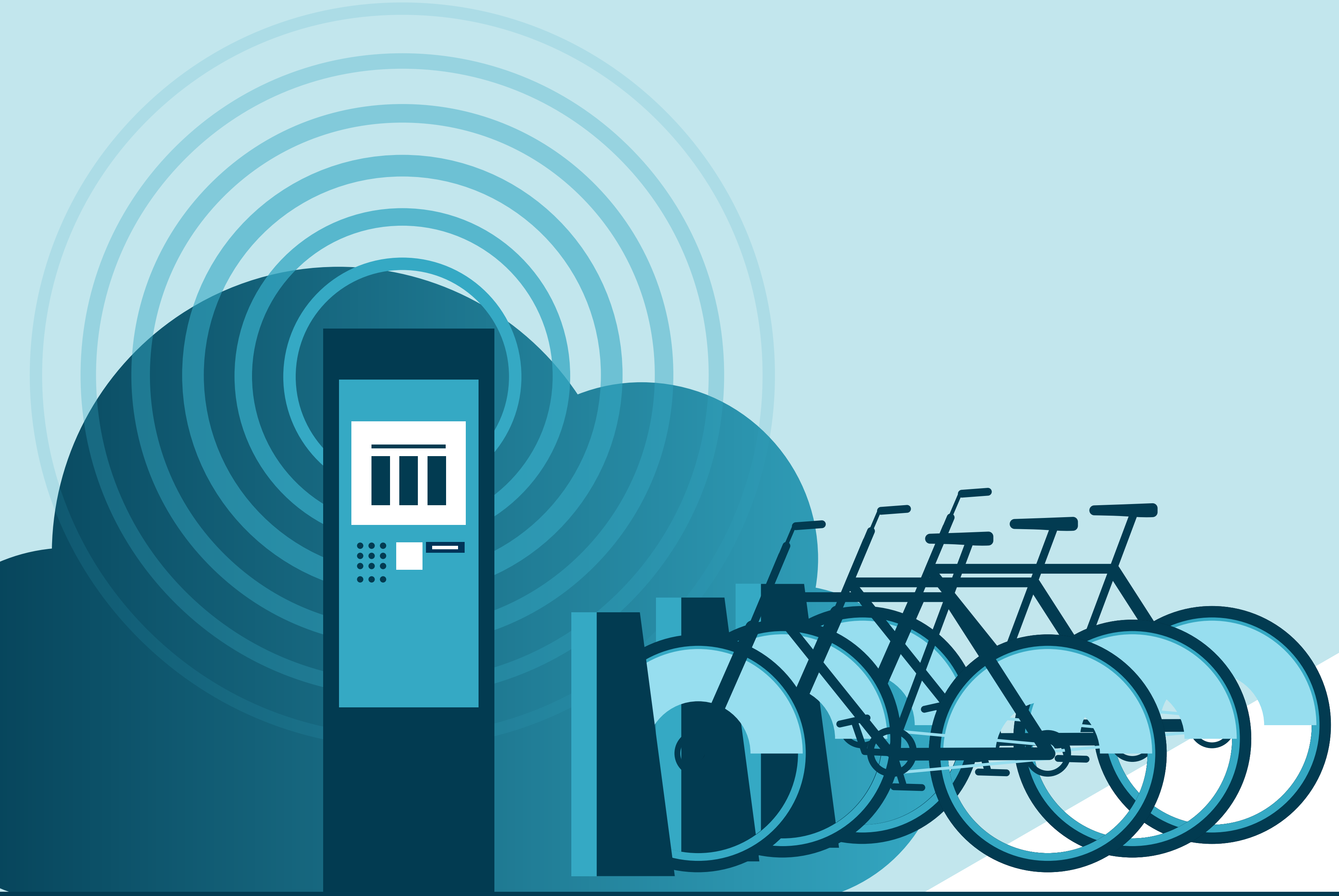
Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Connected Places Cyber Security Principles 101

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

Executive summary



What is this resource?

This resource is designed to be a presentation that local authorities can use to share introductory information on the NCSC's Connected Places Cyber Security Principles (the Principles) with the staff in their organisation.

How should I use it?

The slides in this document and accompanying presenter notes can be used to deliver an introductory presentation to local authority staff to share awareness of the Principles and how to apply them to secure your connected places. The resource can also be included in onboarding packs for new staff.

Who does this resource apply to?

The contents of this resource apply to a broad range of stakeholders within your local authority, from new starters to board members. It is especially relevant to staff who will be involved in the design and maintenance of connected places projects or the procurement of connected technologies.

What will I get out of using this resource?

Connected places projects are looked after by a range of internal teams within a local authority and not all stakeholders will have cyber expertise. This lack of cyber security awareness can make it difficult to embed the Principles into the design, understanding and maintenance of connected places projects.

Using this resource will give teams in your local authority a basic awareness of the Principles. When your teams are thinking of using connected places technology in their business areas, as is increasingly happening, they will know (1) to consider cyber security from the outset and (2) where to look for more detailed information as their project(s) progress.

This Principles 101 resource aims to increase basic connected places cyber security awareness across the authority, not make everyone an expert in cyber security.

City of Westminster

Case study: Westminster City Council (WCC)

Westminster City Council is embarking on a project to develop a Smart City Operating System, which is a modern data platform that aggregates and shares connected places data both internally and externally to deliver economic and social value for the organisation. In the absence of the Smart City Operating System, business areas are aware of the data protection requirements for the project, but there is not the same level of awareness across the organisation for cyber security considerations.

Westminster City Council has run sessions using the Principles 101 resource to raise security awareness across its relevant teams. An early session resulted in a service area and Digital and Innovation (D&I) exploring cyber security in a connected places project previously unknown to D&I.

See Appendix for more on the case study.

Contents

Introduction and definitions

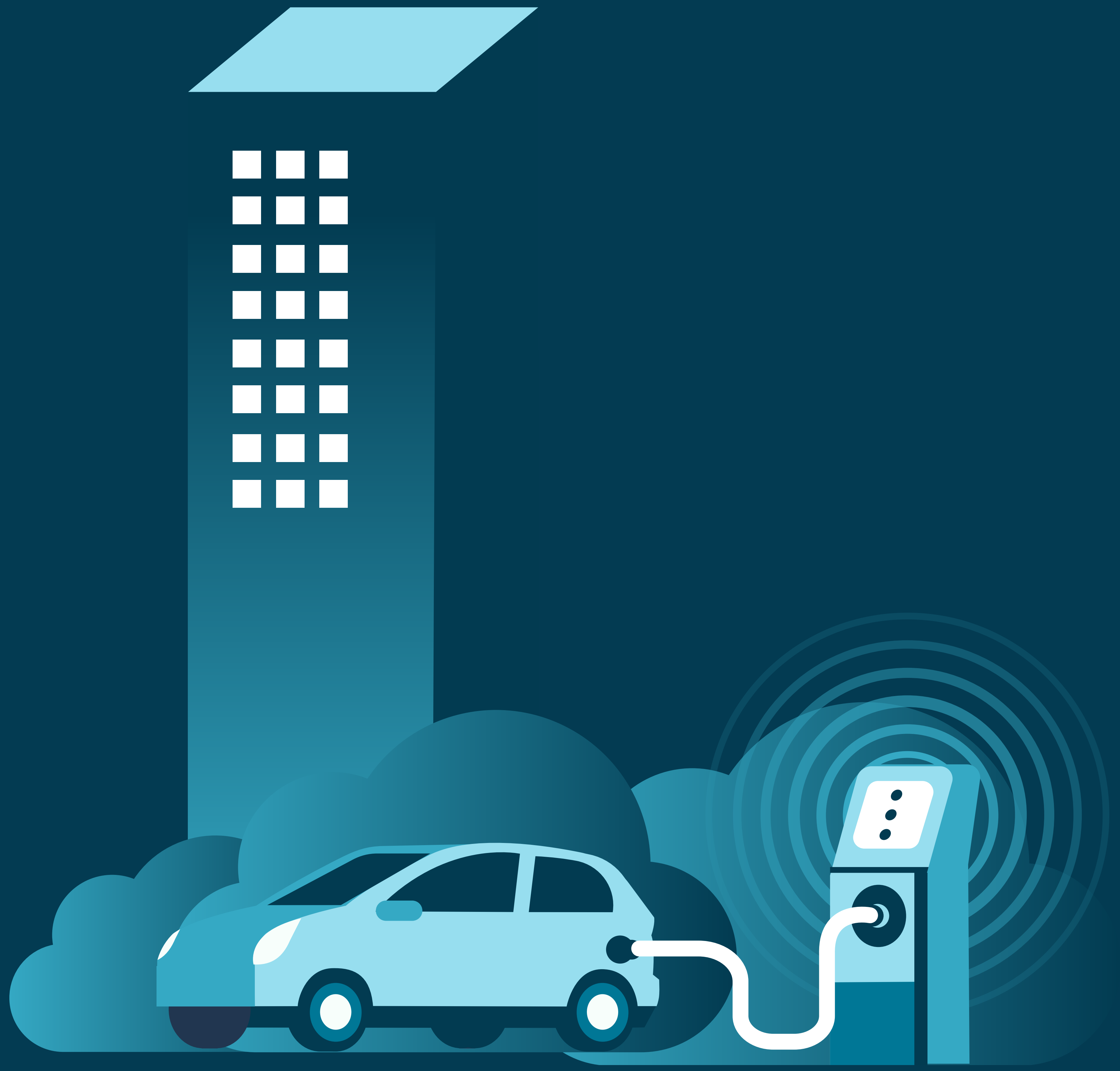
What are connected places?

“The fundamental aim of a connected place is to enhance the quality of living for citizens through collaborative, interactive, and connected technology.

For the purpose of this guidance, a connected place can be described as **a community that integrates information and communication technologies and IoT devices to collect and analyse data** to deliver new services to the built environment, and enhance the quality of living for citizens.

A connected place will use a system of sensors, networks, and applications to collect data to improve its operation, including its transportation, buildings, utilities, environment, infrastructure, and public services.”

- NCSC Connected Places Cyber Security Principles, May 2021

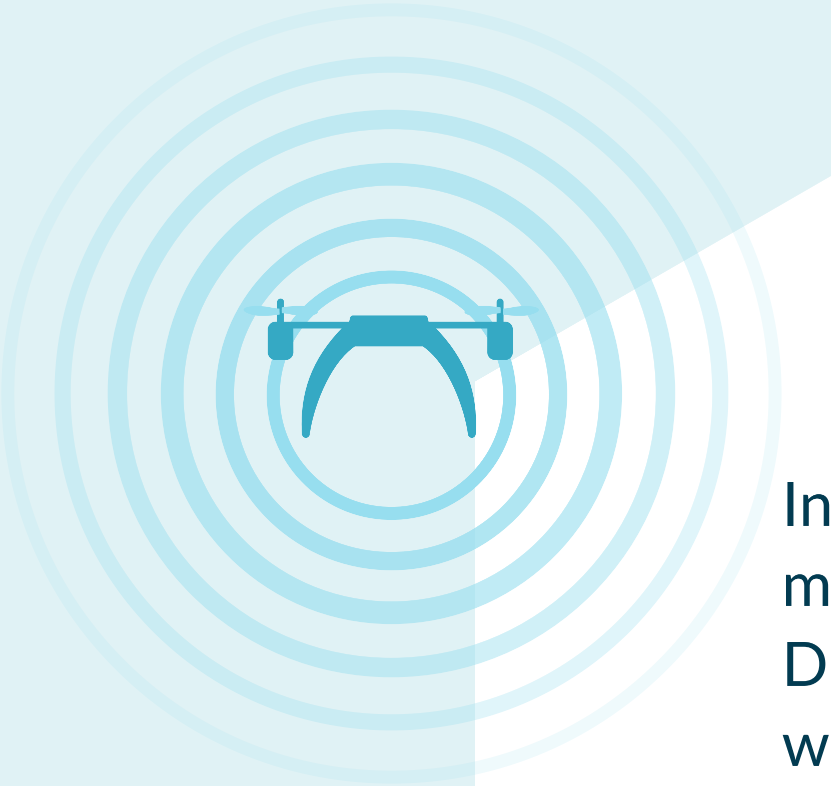


What is cyber security?

“Cyber security is the means by which individuals and organisations reduce the risk of becoming victims of cyber attack.”

“Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it’s difficult to imagine how we’d function without them. From online banking and shopping, to email and social media, it’s more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data and devices.”

- NCSC What is cyber security



In the context of connected places, cyber security is what makes connected places a safe place to live and to work. Designing connected places with an assumption that they will be compromised is a useful approach to ensure that appropriate controls are designed for detecting, protecting against, responding to and recovering from cyber incidents.

It is important to take a holistic approach when securing your connected places, considering personnel, physical and cyber security. Further information about personnel and physical security is available on the CPNI website.

What is the role of DSIT?

Department for
Science, Innovation,
& Technology

The National Cyber Strategy 2022 outlined the Government's objective for the UK to be at the forefront of the secure and sustainable adoption of connected places technology.

DSIT's work contributes to this aim by delivering policy that supports the cyber security of the UK's connected places.

To do so, DSIT's Secure Connected Places team works closely with managers of connected places projects and suppliers of connected places technologies to ensure that communities across the UK can enjoy the benefits of secure connected places.

DSIT created the Secure Connected Places Playbook to complement the NCSC's Principles and support local authorities' connected place cyber security

Connected places threats

Cyber security

As places become more connected, and local authorities become more reliant on this connectedness to provide efficient services to their residents, the risk of hacking, malware and accidental misconfiguration rises. Connected places are attractive targets to malicious actors as they collect, process and store large amounts of data, and an attack on this infrastructure could have a societal-wide impact.

A traffic light prioritisation system that does not authenticate emergency vehicles would be open to anyone changing traffic signals to green, potentially risking lives and damage to vehicles.

In-home health monitoring can be abused for criminal and commercial gain. An attacker could target victims based on their activity patterns. Protecting individuals' privacy is vital.

Electric vehicle chargers should be protected. An attacker could sequence all chargers in the network to draw a large current simultaneously, causing a brownout (a drop in voltage in an electrical power supply system).

Privacy

As data collection is becoming more pervasive, the legal right to individual privacy needs to be protected. With such widespread data collection and correlation, seemingly anonymous datasets can be aggregated to deanonymise individuals.

Data privacy is a very important consideration when deploying connected infrastructure, such as IoT devices within connected places, particularly given suppliers may be exporting and storing data outside of the UK as part of their service.

About the NCSC Connected Places Cyber Security Principles

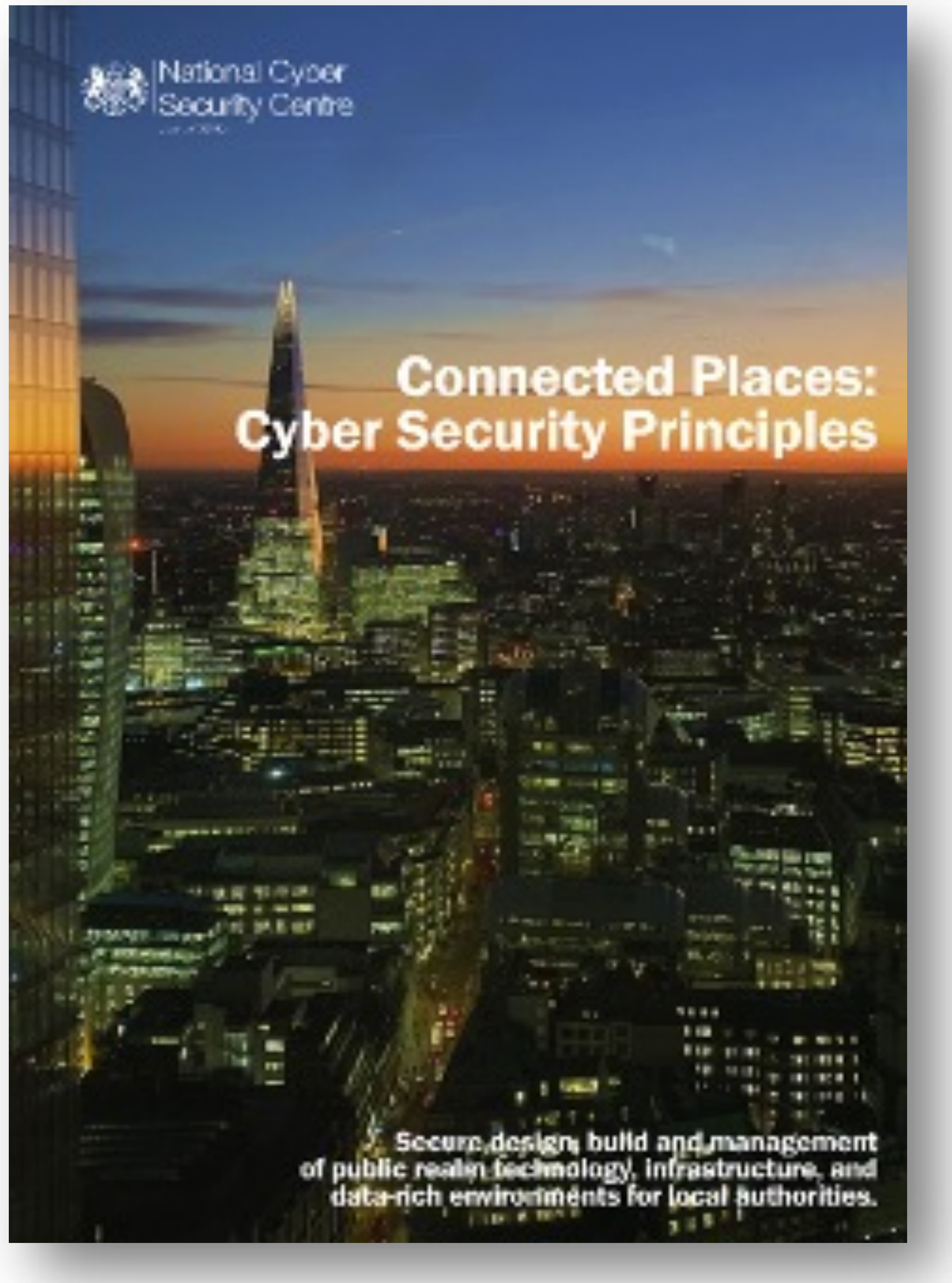
Background

The National Cyber Security Centre (NCSC) released its Connected Places Cyber Security Principles in May 2021.

Whilst the adoption of connected places technology seemed to be increasing, there was a perception that security controls proportionate to the risk were not being considered.

It is principle-based guidance to support local authorities to make better-informed security decisions, not a baseline for compliance.

See the Principles in full here



National Cyber Security Centre

Connected Places: Cyber Security Principles

Secure design, build and management of public realm technology, infrastructure, and data-rich environments for local authorities.

Principles structure

1

Understanding
your connected place

2

Designing
your connected place

3

Managing
your connected place

Understanding your connected place

1. Understanding your connected place and the potential impacts

2. Understanding the risks to your connected place

3. Understanding cyber security governance and skills

4. Understanding your suppliers' role within your connected place

5. Understanding legal and regulatory requirements

It is essential to know your local authority's desired business outcomes
and how these can be affected.

Designing your connected place

6. Designing your connected place architecture

7. Designing your connected place to reduce exposure

8. Designing your connected place to protect its data

9. Designing your connected place to be scalable and resilient

10. Designing your connected place monitoring

Building security in at the start of a project is widely considered more cost effective than having an attack and paying to remediate later.

Managing your connected place

11. Managing your connected place's privileges

12. Managing your connected place's supply chain

13. Managing your connected place throughout its life cycle

14. Managing incidents and planning your response and recovery

As your connected place grows – collecting more data and automating responses – it is likely to become of increasing interest to malicious actors. This increased automation and data sharing will also intensify the risk of cascade service failures across your connected place and its partners. Therefore, a mindset that assumes your connected place will be compromised is essential to being resilient and ensuring the continued provision of services.

Summary and next steps

Connected Places Cyber Security Principles 101: summary & next steps

1

Key take aways

Having completed this resource, you should feel better informed in the way in which the Principles are trying help local authorities improve cyber security across connected places.

You should know that the Principles set out processes and guidance for three stages of connected places projects: understand, design and manage.

You should also have a basic understanding of connected places, their cyber security threats and where to begin looking for more information to help mitigate them.

2

Questions to ask

It is likely you may have outstanding questions as to how to make progress towards implementing these Principles in your connected places such as:

- Where do we start?
- Who is responsible for our connected place?
- Are there existing processes for managing these cyber threats?

We recommend that you discuss these questions with the relevant teams within your organisation.

3

Next steps

This resource serves as an introductory module of the DSIT Secure Connected Places Playbook.

For further guidance on the processes and policies that will help you to secure your connected places, please consult the other resources in the Playbook.

Appendix

How this resource has been used by local authorities

Case study:

Westminster City Council

City of Westminster

Need:

Westminster City Council is embarking on a project to develop a Smart City Operating System which is a modern data platform that aggregates and shares data both internally and externally to deliver economic or social value for the organisation. In the absence of the Smart City Operating System, service lines are aware of the data protection requirements for the project, however, cyber security considerations do not currently share the same level of awareness across the organisation.

Solution:

Using this resource, Westminster City Council can deliver basic training presentations on the Principles to staff to provide a broad level of understanding of connected places cyber security. This would prompt their staff to ask questions and seek answers about the cyber security of their connected places projects. This presentation could also be embedded as a mandatory exercise at the kick-off for connected places projects to ensure that cyber security risks are appropriately addressed and mitigated at the outset. The Connected Places Cyber Security Principles 101 resource provides a high-level overview in a presentation format that allows local authorities to give a baseline understanding to their staff.

Outcome:

Westminster City Council has run sessions using the Principles 101 resource to raise security awareness across its relevant teams. An early session resulted in a service area and Digital and Innovation (D&I) exploring cyber security in a connected places project previously unknown to D&I.

Glossary of terms

Term / acronym	Definition
Architecture	The designed structuring of something e.g. an agreed set of components for IT systems
Connected places	Connected places are a communities that integrate information and communication technologies and Internet of Things devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens. Connected places will use a system of sensors, networks, and applications to collect data to improve its operation, including its transportation, buildings, utilities, environment, infrastructure, and public services
Connected technology	Products with technology built in that allow them to connect with their environment and other products, for instance, internet of things devices
Cyber security	The practice of protecting computer systems from attack
DSIT	Department for Science, Innovation & Technology
IoT	The Internet of Things describes physical objects with sensors, processing ability, and software that connect and exchange data with other devices and systems over the Internet or other communications networks
NCSC	National Cyber Security Centre
The Principles	The NCSC's Connected Places Cyber Security Principles
System	A group of people, processes and technologies that conform to a policy to achieve a desired objective
System approach	A philosophy that considers a problem as the result of, or to be solved by, a system

Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Please contact secureconnectedplaces@dcms.gov.uk with any questions or feedback on these resources.

This Playbook was produced in collaboration with:

plexal DAINTTA Configured THINGS

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION