National Protective Security Authority

ADVICE NOTE

Connected Places: related legislation, regulations & guidance

Introduction

The information in this document does not constitute legal advice. It is provided in support of the guidance contained in PAS 185:2023 to draw to the attention of decision-makers responsible for connected places. The legislation listed below is set out in alphabetical order and is not intended to be exhaustive. Users of this document should take appropriate legal advice where any of the legislation or regulations applies to assets and to asset data or information under their control.

1. Building Safety Act 2022

The Act provides for building safety information to be disclosed to residents and owners of residential units in a higher-risk building, and to request additional information on beyond that which they would automatically receive. When connected places authority collects, processes or stores building safety information, sufficient protocols should be in place to control access to maintain the security of the building or residents. Where the building safety information includes personal information, it should be protected in accordance with the provisions of the Data Protection Act 2018.

NOTE In disclosing building safety information care should be taken to ensure that the security of both the building and the security of other buildings in the vicinity are not compromised. For example, disclosure of information about a technical system that controls sprinklers in a building, where disabling the sprinkler system could have a negative impact on surrounding buildings because of the risk of fire spread. In this example, appropriate security-minded measures should be implemented to protect and prevent unauthorised disclosure of information about the technical system.

2. Computer Misuse Act 1990

Connected place decision-makers should apply a security-minded approach in their specification, design, operation and maintenance of data and information systems that form part of any connected place, to ensure that citizens, personnel, professional advisors, contractors, and suppliers do not inadvertently commit offences when fulfilling their contracted duties.

NOTE Offences can arise where an individual accesses data or information when they lack the requisite privileges or authorization. The access might include viewing, printing, moving data or information or altering files or database records.

3. Crime and Disorder Act 1998

Connected place decision-makers should apply a security-minded approach to considering the crime and disorder implications when exercising its functions.

NOTE Section 17 of the Crime and Disorder Act places a duty on an authority to exercise its functions with due regard to the likely effect of the exercise of those functions on, and the need to do all it can to prevent, crime and disorder in its area.

4. Data Protection Act 2018

Connected place decision-makers should apply a security-minded approach to handling, storage and use of personal data that forms part of the connected place.

NOTE 1 The Data Protection Act regulates the use of personal data and could apply to asset information, whether held in electronic or paper form, where it includes any set of information

relating to individuals. The need for identification and protection of personal data is addressed in Clause 8 of PAS 185:2023.

NOTE 2 The provisions of the DPA (2018) implement the provisions of General Data Protection Regulation (GDPR) (Directive 95/46/EC).

5. Environmental Information Regulations 2004

Where a connected place authority holds information that falls within the scope of the Environmental Information Regulations 2004, it should release asset information, as part of its publication scheme and on request, on a risk-based, security-minded basis. It should inform personnel handling such requests of the types of information to be withheld.

NOTE The Environmental Information Regulations 2004 provides public access to information about the environment held by public authorities by:

a) *obliging public authorities to proactively publish certain information about their activities in accordance with their publication scheme, and*

b) *entitling members of the public to request information from public authorities.*

The Regulations cover any recorded information held by the public authority that falls within the definition of environmental information and can also apply to environmental information that another person or organization holds on behalf of the public authority. Environmental information typically covers information about land development, pollution levels, energy production, and waste management, and includes financial information where it relates to the costs of redeveloping land and constructing a new built asset.

Where a connected place authority is the employer on a construction project or asset owner regarding a built asset, it should consider what, if any, asset information is to be published as part of its publication scheme, the extent to which members of the public might be provided with information in response to Environmental Information Regulations 2004 requests, and the exemptions that exist.

6. Freedom of Information Acts

The Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002

Connected place decision-makers should, on a risk-based, security-minded basis, consider what asset data or information might be released as part of the authority's publication scheme and on request. Connected place decision-makers should make the personnel handling such requests aware of the types of information to be withheld.

Where a connected place involves data and information processed by more than one public authority or legal entity covered by the FoI legislation, the connected place decision-makers should agree appropriate processes to ensure that sensitive information.

NOTE The Freedom of Information 2000 and the Freedom of Information (Scotland) Act 2002 provide public access to data and information held by public authorities, by:

a) *obliging public authorities to proactively publish certain data and information about their activities in accordance with their publication scheme, and*

b) *entitling members of the public to request data and information from public authorities.*

Together the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 cover any recorded information that is held by a public authority in England, Wales, and Northern Ireland, and by UK-wide public authorities based in Scotland.

Where a connected place authority is the employer on a construction project or asset owner regarding a built asset, it should consider what, if any, asset data or information is to be published as part of its publication scheme, the extent to which members of the public might be provided with information in response to freedom of information requests, and the exemptions that exist.

7. Government Security Classifications

Where applicable, a connected place authority should comply with the Government Security Classifications policy with regards to all data and information that it collects, stores, processes, generates or shares, to own, procure, operate, or maintain connected place services and built assets, including data and information received from, or exchanged with, external parties both within and outside its supply chain.

NOTE 1 Compliance with this policy might require specific security measures to be imposed regarding the access to, storage and processing of data and information, particularly where there are significant volumes of official data or information or where some of the data or information requires specific controls and security measures.

NOTE 2 Government Security Classifications apply to all data and information that the government collects, stores, processes, generates, or shares to deliver services and conduct business, including data and information received from, or exchanged with, external partners.

NOTE 3 The application of Government Security Classifications to all data and information that the connected place collects, stores, processes, generates or shares to deliver services and conduct business, irrespective of whether it comprises central government information, is good security practice.

8. Local Government Transparency Code (2015)

Connected place decision-makers should adopt a security-minded approach when publishing objective, factual data and information, on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

NOTE It is important that connected place decision-makers strike the right balance between making data and information available, thus delivering the transparency that is the foundation of

local accountability, whilst restricting access to sensitive data and information that could jeopardize or undermine the safety and security of assets, services, and citizens.

9. Network and Information Systems Regulations 2018 (SI 2018/506)

Connected place decision-makers should understand the scope of SI 2018/506 Directive EU 2016/1148 (the NIS Directive) and where applicable apply a security-minded approach to the design and operation of essential connected place services.

NOTE 1 The Network and Information Systems Regulations (NIS Regulations) provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services.

NOTE 2 The Regulations provides legal measures to boost the overall level of cyber security across sectors which are vital for the economy and society, such as energy, transport, water, health, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified as operators of essential services should take appropriate security measures and to notify serious incidents to the relevant national authority. Key digital service providers (search engines, cloud computing services and online marketplaces) are also required to comply with the security and notification requirements under the Regulations.

NOTE 3 Further advice on NIS-related cyber security is available here [https://www.npsa.gov.uk/cyber-security],

10. Official Secrets Act 1989

Where official data or information is held in paper or electronic form, a connected place authority should apply protective measures in accordance with the UK Government guidance on information security.

NOTE The Official Secrets Act 1989 applies to the protection of official information. Where the data or information relates to the safety and/or security of the connected place, serious and organized crime, or part of the critical national infrastructure, it might be sensitive and might be covered by the Official Secrets Act. Where the data or information is covered by the Official Secrets Act, additional protective measures might be required in accordance with the Government's guidance on information security.

11. Planning and Compulsory Purchase Act 2004

If a connected place authority submits a planning application which is handled by a planning inquiry, it should request that the provisions of Section 80 of the Planning and Compulsory Purchase Act (2004) be applied to all security-sensitive information regarding the built asset or planned built asset.

NOTE Section 80 of the Planning and Compulsory Purchase Act 2004 deals with the arrangements for planning inquiries where matters of national security are at issue. While, in general, all oral evidence at planning inquiries should be heard in public and all documents should be open to public inspection, there is an exception when there would be public disclosure of information relating to national security or to the security of any premises or property, and that disclosure would be contrary to the national interest.

12. Privacy and Electronic Communications Regulations 2003

Connected place decision-makers should be aware of the Privacy and Electronic Communications Regulations 2003 and consider whether any of the provisions apply to their built asset and IT and communications systems, and if so, implement appropriate measures to instil compliance.

13. Public Records Act 1958 and Public Records Act 1967

Connected place decision-makers should consider what information is required to be retained for public record purposes. Where a built asset in public ownership or use has a lifecycle greater than 30 years, the connected place authority and asset owner should, on a risk-based, security-minded basis, consider what asset information might need to be sealed for a longer period to prevent compromising the security of the built asset. Where the data is personal data, the connected place authority should consider the potential security risks associated with making such records public.

NOTE Attention is drawn to the Public Records Act 1958, the Public Records Act 1967, and the data protection legislation and regulations regarding the publication of personal data.

14. Re-use of Public Sector Information Regulations 2005

A connected place authority should apply a security-minded approach when considering what data and information should be made available for re-use, and the extent to which the connected place data and information is exempt from re-use.

NOTE Public authorities should consider the security implications of making connected place data and information available for re-use. Whilst individual items might not pose a threat, aggregation, including correlation of data and/or information supplied by different public bodies, could reveal sensitive operational information and capabilities. Where security considerations might be applicable, the public authority should not identify the data or information as available for re-use.

15. Sensitive information in planning applications

Where a planning application contains sensitive data or information, a connected place authority should work with the construction employer or asset owner to apply a security-minded approach to the handling of the application. The planning authority for the connected place should work with the construction employer or asset owner to limit the data and information available on the open planning register, with sensitive data and information being subject to special handling arrangements.

NOTE 1 Planning applications from bodies such as the diplomatic community, defence, security and law enforcement organizations, and owners of critical national infrastructure might contain sensitive data or information, which the local planning authority should consider, but which should not be made available on the planning register.

NOTE 2 Before accepting or registering a planning application, the connected place planning authority should discuss the status of sensitive data and information relating to a proposed development with the construction employer or asset owner.

Further information can be found at:

https://www.gov.uk/guidance/crown-development#sensitive-information-in-planning-applications