Delivering Valuable Data:

An Interoperability Code of Practice for Technologies in the Built and Managed Environment

Version 1.0
April 2023

Table of Contents

1 Introduction

Interoperability – the ability to exchange and use information securely, ensuring that information is independent of the technologies used to deliver it[1] – is vital if owner-operators wish to maximise the value of their physical assets in the built and managed environment.

Owner-operators need information about their buildings, infrastructure or other assets to be findable, accessible, interoperable and reusable throughout the lifecycle of those assets. This information is an important asset itself, with intrinsic long-term value, critical for operation, maintenance and disposal of the asset, and for regulatory and other portfolio purposes.

However, poor interoperability of information in the built and managed environment sector has been a perennial issue. Its roots include the silo-based, highly fragmented and often adversarial nature of the industry, which frequently focuses on short-term outputs or deliverables, rather than whole-life outcomes, and the slow pace of digital adoption. Inadequate interoperability affects industry productivity, adding time and costs at all stages of the life cycle of physical assets, with most of the costs borne by owner-operator organisations. Where these are public sector organisations, this means costs to taxpayers; in the UK, as elsewhere, poor interoperability reduces the value of information, diminishing industry's ability to deliver for the public good.

As a result, to help deliver better whole-life outcomes, achieving better interoperability has become a stated aim of the UK Government's construction strategy, demanded in the *Construction Playbook*[2] and the *TIP Roadmap to 2030*.[3] Improving interoperability also contributes to ambitions of greater sharing of better data across government, supported by national digital, data, and geospatial strategies, by guidance in the *Digital, Data and Technology Playbook*[4] and the Central Digital and Data Office (CDDO) Technology Code of Practice,[5] and by a growing range of international standards and protocols intended to support secure exchange and use of electronic information.

This Code of Practice (CoP) outlines the principle of interoperability and five principles that underpin achieving and maintaining interoperability in the built and managed environment. These five underpinning principles comprise:

a. **longevity** – enabling better long-term findability, access, reuse and exploitation, and therefore continued value, of information;

b. **security** – maintaining necessary security, confidentiality and privacy protections, while maximising opportunities for sharing non-sensitive information for the public good;

c. **information value** – enhancing the value of information created, managed and shared by technology-using professionals;

d. **information ownership** – ensuring enduring ownership and control by asset owner-operators of valuable data about the assets they own; and

e. **competition** – promoting fair competition between technology providers (and indirectly among supply chain users of technologies).

The initial focus of the CoP is on supporting the whole life needs of industry clients – in particular, asset owner-operators in the public sector, but recognising private sector clients have similar needs.[6]

By setting principles that should be adopted by information technology providers, this CoP highlights their critical role in helping asset owner-operators and their supply chains to manage contractual information exchanges – an activity that requires input from both individual users and the contractual parties. The CoP aims to help industry respond to new economic, environmental and social pressures, and to build sustainable foundations for future technological opportunities.

The CoP builds on over a decade of UK experience of wider digital advancement, including in relation to Building Information Modelling (BIM). With digital transformation still in progress, this first edition of the CoP has adopted a 'minimum viable product' or incremental approach, setting foundations and indicating likely future steps. It has been developed by a working group comprising individuals from technology vendors, supply chain organisations and asset owner-operators. A draft was shared during a public consultation exercise in January and February 2023, and was updated in light of feedback received.

[1] *GIIG Glossary* (November 2022). The emphasis is on enabling information exchange and use, then with appropriate security.
[2] Cabinet Office, *The Construction Playbook: Government guidance on sourcing and contracting public works projects and programmes*, v1.1 September 2022.
[3] Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. Annex B: The Information Management Mandate. In this document, it is hereafter referred to as the *TIP Roadmap to 2030.*
[4] Cabinet Office, *Digital, Data and Technology Playbook*, March 2022
[5] Central Digital and Data Office, Technology Code of Practice, last updated November 2021.
[6] Better interoperability is also urged in *Trust and productivity: The private sector construction playbook* from the *Construction Productivity Network (2022)*

2

Section 2

Objectives and applicability

2.1 Objectives

The CoP has the following objectives:

a. to enable built and managed asset owner-operators (and their advisers), supply chain members and technology providers and other stakeholders, to create and implement information management systems capable of interoperable information exchange in non-proprietary formats[7] based on open standards. This allows recipients full access and use to information in other technologies, for immediate use and for future re-use.

b. to help government clients, their advisers, suppliers and technology providers meet *Construction Playbook*[8] and *TIP Roadmap to 2030* requirements (including the UK BIM Framework and emerging Building Safety Act regulations): "...a digital mechanism for defining ...information requirements and then procuring, receiving, assuring, and immutably storing, via a system of record, the information that it procures."[9]

c. to provide clear practical guidance so that teams can understand how interoperability relates to their job roles and responsibilities in planning, designing, creating and maintaining built asset(s) and the surrounding built and managed environment.

d. to provide guidance that is easily understood and usable by a wide range of individuals from both technical and non-technical backgrounds.

e. to help establish information quality, availability, alignment and interoperability of sector datasets; these can catalyse innovation and add business value, and enable more efficient (and thus less costly) construction approaches such as Modern Methods of Construction and off-site assembly,[10] and

f. to encourage integrated information management across the whole life of built or managed assets, and across portfolios or collections of multiple assets.

[7] Data in a proprietary format typically relies on specific software to read the data, and cannot be read without that software.
[8] Cabinet Office, *The Construction Playbook: Government guidance on sourcing and contracting public works projects and programmes*, v1.1 September 2022, pp.23-24.
[9] Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. Annex B: The Information Management Mandate, p.57.
[10] KPMG/Atkins (2021) *The value of Information Management in the construction and infrastructure sector: A report commissioned by the University of Cambridge's Centre for Digital Built Britain*, s 4.3.2 'The role of Information Management in helping to drive social value, pp31-32.

2.2 Primary audiences

The primary audiences for this CoP are, in this order:

a. **Providers of information management technologies** used to support delivery of information relating to built and managed assets;

b. **Owner-operators:** organisations that need to procure information relating to the assets they own, operate, occupy or otherwise use – often, they may procure information management technologies direct from technology providers, and/or procure services including information management services from supply chain members (c, below); and

c. **Supply chain organisations:** typically consultants and contractors contracted by clients or owner-operators to provide services, including technical services relating to planning, design, construction or operation and maintenance of buildings or other physical asset(s).

In addition to its primary audiences, the CoP may also relate to other groups including:

a. Membership organisations of which professionals in sections a) to c) are members;

b. Educational bodies including universities and providers of continuous professional development services and materials used by professionals in sections a) to c); and

c. Regulators, including bodies responsible for built or managed asset information compliance.

3

Section 3

Interoperability

3 Interoperability

Information should be capable of secure exchange between two or more systems so that it can be used and managed. It should not be dependent on the technologies or services used to produce or process it.

This is the most important principle of the CoP, core to maintaining and maximising the value of information. Improving interoperability in the built and managed environment sector has been an objective of the UK Government since 2011.[11] It is a current requirement of UK construction strategy, particularly highlighted in the *TIP Roadmap to 2030* and in the *Construction Playbook*. Both refer to the UK BIM Framework which, citing ISO 19650,[12] distinguishes between proprietary and open data (data available/visible to others and that can be freely used, re-used, re-published and redistributed by anyone). In this Code of Practice, the focus is on making data available in non-proprietary formats, or formats that are published as open standards.

Today, where a government department or agency is buying technology, the principle of interoperability is also covered in the *Government Functional Standard GovS 005: Digital, Data and Technology*,[14] the *Digital, Data and Technology Playbook* and the CDDO Technology Code of Practice. The *DDaT Playbook's* key policies include adoption of non-proprietary data formats and use of interoperable data. It says "The ability to exchange and share information and data between contracting authorities and suppliers and across government is key for long-term success. ...Operating in this consistent way will allow the interoperability between systems which fuels innovation."[15] Focusing on procurement of technologies, the *DDaT Playbook* stresses the need for interoperability:

> "Government's information assets, including data, should be able to be easily exchanged across platforms to make efficient use of the data we own. Contracting authorities should ensure that all contracts, including for commercial off-the-shelf (COTS) software, enable data extraction in a common format and IP and licencing requirements should be considered to ensure accessibility and transparency."[16]

The CDDO Technology Code of Practice Point 4, 'Make use of open standards', urges use of open standards[17] technology so that it is easier to expand and upgrade, and to ensure it communicates with other technology.[18] The CDDO also advises Government buyers of technologies: "You should manage your data as an asset that is independent of any technology or service. This will involve using data standards to help you store your data so other government organisations can find and reuse it."[19] This will help Government to maximise the value of its collective information and reduce information value depreciation over time.

3.1 What the interoperability principle means for technology providers

Technology providers should ensure that their products or services support the exchange of non-proprietary information without loss, amendment, mis-interpretation or additional work for users, so that the integrity and value of information is not compromised.

While information will often be initially created and developed using proprietary software or services, when a supplier needs to exchange information with a contracting authority or other supplier, that information should be deliverable in an agreed non-proprietary form based on open FAIR principles,[20] so that it is also easily and immediately findable, accessible and reusable by the recipient. Recipients should not have to use a proprietary software to find, access or reuse information provided to them (this does not preclude the maintenance of records in both native and open forms where there is any uncertainty).

[11] Government Construction Client Group, BIM Working Party Strategy Paper, *BIM: Management for value, cost and carbon improvement*, March 2011: "Government as a client can derive significant improvements in cost, value and carbon performance through the use of open shareable asset information."

[12] ISO 19650-1, clause 6.1 states that information exchanges should be done using open standards whenever possible. This is also reiterated within ISO 19650-2, clause 5.1.6.

[13] UK BIM Framework, ISO 19650 Guidance B: Open data, buildingSMART and COBie, s 1.2.

[14] *Government Functional Standard GovS 005: Digital, Data and Technology*, s 2 Principles: "When creating or providing and using digital services, government organisations and individuals shall ensure... [point 7:] Digital and technology components are designed using mandatory government open standards where needed; and are adaptable, interoperable and shareable."

[15] Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.4.

[16] Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.61.

[17] The *GIIG Glossary* (November 2022) defines an open standard as "A standard for which the specification or schema is publicly available, where the drafting and maintenance of the specification is open to all interested parties and is consensus-based, and where use of the resulting standard is royalty-free." This draws on a Cabinet Office Policy paper: *Open Standards principles* (updated 5 April 2018)

[18] CDDO Technology Code of Practice, *Point 4: Make use of open standards*.

[19] CDDO, *Manage your data for access and reuse*, (November 2020): see also CDDO advice in *Make better use of data*, updated March 2021.

[20] As the UK's Geospatial Commission is developing a geospatial code of practice incorporating the FAIR principles (see *How FAIR are the UK's National geospatial data assets? Assessment of the UK's national geospatial data assets*), this Code of Practice has incorporated the FAIR approach. See also www.go-fair.org

3.2 Related technical requirements:

a. **Open standard formats and schemas –** Software should apply British or internationally recognised open standards for the rendering of common information in machine-readable formats – for example:

- ISO 8601:2004 for the presentation of dates and times
- World Geodetic System 1984 (WGS84), European Terrestrial Reference System 1989 (ETRS89) and OSGB36 (Ordnance Survey of Great Britain 1936 Datum – used in many UK data sets) standards for consistent exchange of location point information
- GeoJSON format for encoding and exchanging location information
- UK GEMINI 2.3 for geographic metadata
- ISO 3166 for country codes
- BS 7666-2 for property and street identification in Great Britain through unique property reference numbers (UPRNs) and unique street reference numbers (USRNs)[21]
- ISO 16739-1:2018 - Open relational data schemas (inherently more persistent than proprietary files) such as IFC (Industry Foundation Classes) and specific use cases such as Construction Operation Building information exchange (COBie)
- ISO 12006-2 for classification (Uniclass)

b. **APIs (application programming interfaces)** – Machine-level access to asset-related information management systems should, for example, be via extendable scripted RESTful or GraphQL APIs. The *Digital, Data and Technology Playbook* says: "APIs [should] conform to Central Digital and Data Office API technical and data standards, satisfy the requirements of the Technology Code of Practice…, and [be] well documented."[22] It stipulates APIs "should be used to enable effective data sharing… in interoperable, reusable and open formats. …This is also enabled by the use of open data standards rather than bespoke ones."[23] The CDDO guidance also:

- advocates the OpenAPI Specification as a standardised way of describing RESTful web APIs. OpenAPI – specifically, OpenAPI version 3 – is recommended by the government Open Standards Board[24] to help government organisations be consistent in describing RESTful APIs, to generate accurate up-to-date API reference documentation, and to validate, version, maintain and update generated documentation
- provides guidance on good practice to follow in designing, building, hosting and operating secure APIs, including provision of i) data level security (ensuring users only have access to data they are authorised to see) and ii) application level security (ensuring only authorised users can access the API)

Also in relation to APIs, see ISO/IEC 20802-1:2016 - the Open Data Protocol (OData, an open protocol that allows the creation and consumption of queryable and interoperable REST APIs in a simple, standard way) and ISO/IEC 20802-2:2016 - the OData JSON format.[25]

Note: This section on the CoP's principle of interoperability should be read in conjunction with the following section.

[21] UPRNs and USRNs are available as open data under Open Government License from the Ordnance Survey.
[22] Central Digital and Data Office, *API technical and data standards* (updated 11 July 2022); Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.4; see also p.61.
[23] Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.84.
[24] Central Digital and Data Office, *Describing RESTful APIs with OpenAPI 3* (updated 7 August 2020).
[25] OData has been developed through the international *OASIS Open group*.

4

Section 4

Principles

4 Principles

Five principles underpin achieving and maintaining interoperability in the built and managed environment, namely:

1. **longevity;**
2. **security;**
3. **information ownership;**
4. **information value; and**
5. **competition.**

These principles reflect demands in UK Government technology guidance and in built and managed environment guidance (for example, the Construction Playbook, TIP Roadmap to 2030 and UK BIM Framework). For each principle, the implications for technology providers are set out, and related technical requirements are given (some technical requirements span multiple principles). These may form the basis for future assessment of technologies by clients during procurement processes.

4.1 Longevity

Information should remain appropriately accessible and useable across asset owner-operator systems, including for audit trail, provenance or regulatory purposes, supporting decision-making activities and providing ongoing value through the whole life of the physical asset(s) to which it relates.

Interoperability is not a short-lived or temporary requirement, nor is it solely related to asset delivery or operational activities (for example, information may be contractually required for activities as part of a feasibility or planning phase for assets yet to exist, or it may be related to Organisational Information Requirements, OIRs). Information may be progressively handed over during delivery of a new asset, or it may be provided during the handover of the physical assets to which it relates. It should then be capable of reuse throughout the lifecycle of those assets for information purposes relating to occupation, operation or change of ownership, through to end of life. In particular, information may be reused for anticipated activities such as regular maintenance or inspections, or for unpredicted ‘trigger events’ that may result in repairs, replacements or other required works.[26]

[26] See UK BIM Framework guidance, *ISO 19650 Guidance 3: Operational phase*, s 4.2

[27] UK BIM Framework, ISO 19650 Guidance B: Open data, buildingSMART and COBie, s 1.1.

[28] UK BIM Framework, ISO 19650 Guidance B: Open data, buildingSMART and COBie, s 1.2.

[29] Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. The Information Management Mandate is in Annex B

Information purposes may relate to individual assets or to both concurrent and retrospective use at a portfolio, pan-organisational, pan-government or pan-industry level; information purposes may also relate to future contractual, warranty or other legal or regulatory compliance needs. Ensuring that information remains findable, accessible, interoperable, reusable and of value is therefore critical for owner-operators and to other stakeholders (supply chain organisations will also need to retain access to some information for contractual, other legal and regulatory compliance purposes). To enable all these information purposes to be fully carried out, information should not be dependent upon any proprietary technologies or data formats.

The UK BIM Framework notes "information needs to remain accessible and interpretable for the whole life of an asset. Without considering the structure of this information, there is a risk that it will not be interoperable."[27] It then underlines the need for non-proprietary data and underlines its use for archival purposes.

> "... this distinction is significant for archiving purposes because it will affect how to record and store information. Assets, including building and infrastructure works, can be designed and constructed for significant lifespans. There is no guarantee that future software solutions will have the ability to access and interpret proprietary information about these assets. Using ... [non-proprietary] data will resolve this issue."[28]

The *TIP Roadmap to 2030* requires clients to "apply ...governance and rigour to the maintenance of its information, to ensure that it provides **ongoing value and benefits to the client organisation.** This will include the ability to share and exploit information, and also make information available for regulatory purposes" (emphasis added).[29]

In relation to building safety regulatory purposes, the Department of Levelling Up, Housing and Communities (DLUHC) 'Golden Thread' principles highlight the need for longevity:

> "**9. Longevity/durability and shareability of information:** the golden thread information needs to be formatted in a way that can be easily handed over and maintained over the entire lifetime of a building. In practical terms, this is likely to mean that it needs to align with the rules around open data and the principles of interoperability – so that information can be handed over in the future and still be accessed."

Organisations should therefore work with technology providers to ensure long-term access to information. In respect of the Building Safety Act, further UK Government guidance is to be published and will include advice on longevity/durability and "practical details to support implementing Common Data Environments and effective information exchange and interoperability."[30] This Code of Practice should be updated in light of this guidance once it is published.

[30] *Building Regulations Advisory Committee: golden thread report*, July 2021, s4.6. In s.5 of the report, 'What should industry be doing now?' BRAC highlighted the golden thread "as part of the growing and widespread recognition that good quality, verifiable and maintained data delivers immense 'value' by providing solid insights to support decision making. In short, the golden thread does not sit in isolation, but forms part of a broad national developing ecosystem of digital and data centric tools which harness the power of data to deliver benefits to all. This journey continues and key work includes embedding the UK BIM Framework, delivering data interoperability between systems and building projects, and taking forward the National Digital Twin Programme." (emphasis added)

4.1.1 What the longevity principle means for technology providers

Technology providers should ensure that their products or services support the continued findability, accessibility, interoperability and reusability of information – including for audit trail, provenance or regulatory purposes – throughout the lifecycle(s) of the asset(s) to which it relates.

While information will often be created and developed using proprietary software or services, when a supplier is required to exchange information with a contracting authority or other suppliers, it should be delivered in a non-proprietary open standards-based data format. Then – subject to the continued development, support and adoption of the relevant open standards – it will remain findable, accessible, interoperable and reusable for future information purposes for as long as required.

Moreover, technology providers should ensure that such information exchanges also preserve historical metadata relating to the information's original creation and its subsequent management and use. Where technology providers provide long-term information management services to a contracting authority or supplier, they should also guard against unauthorised access, use, disclosure, modification or destruction of the information *(see 4.2: security, below)*, and guard against disruption or non-availability of the services including due to liquidation.

Technology providers should also ensure that new products or services are backward compatible. In a software context, this would allow data created in a previous version of an application to be findable, accessible and reusable in a new version of the software (this will, of course, be less of an issue if the software supports open standards – *see 3: interoperability, above*). Particularly where technology providers provide long-term information management services to a contracting authority or supplier, this may also require consideration of archival or data retention policies, and digital preservation and/or migration processes.

a. **Open standard formats and schemas** – *See*

4.1.2 Related technical requirements

3.2 a) above.

b. **Immutability** – All containers (named persistent sets of information retrievable from within a file, system or application storage hierarchy), their contents and associated metadata, and any extracted data, should be immutably held while within an information management system together with its source provenance (including evidence of its integrity). Any change should generate a new separate but associated provenance.

c. **Metadata** – All containers added into an information management system should have fully defined metadata conforming to defined configurations.[31] Any undefined or unreferenced metadata values should cause the container committal to be rejected.

d. **Workflow** – All containers added to an information management system should trigger defined configurable workflows, notifications and other activity, including triggering API calls to external systems, based on specific container metadata values or combinations.

e. **Identity** – All containers added into an information management system should be uniquely identified. All extracted data, notifications, discussions, workflows and other activity, should be referenced back to the unique container identity.

f. **Timestamps** – All containers added into an information management system should be UTC time stamped at the point of committal into the system.

g. **Versioning** – All containers added into an information management system should be versioned against a defined aggregation of container metadata. New container versions should be assigned a unique sequential number based on order of arrival. This is different to revision metadata set by the presenting party.

h. **Provenance** – All containers added into an information management system should hold container identity, source account, datetime and source IP as an immutable record of provenance.

i. **Backward compatibility** – As and when new versions of software products or services are released, they should allow information created in a previous version to be findable, accessible and reusable in the new version of the software.

j. **Information segregation/federation** – Information (containers) should be segregated into different named subsets accessible to users or groups with different levels of security responsibility. When information is federated, those with elevated security credentials will be able to see all authorised levels; those with lower security credentials, will see only what they are authorised to view.

[31] See UK BIM Framework *ISO 19650 Guidance C: Facilitating the CDE (workflow and technical solutions)*, edition 3, November 2022.

4.2 Security

Information should be managed so that it maintains necessary security, confidentiality and privacy protections while maximising opportunities for appropriate sharing of non-sensitive information for the public good.[32]

Information should be managed to prevent unauthorised access, modification, destruction, disclosure, or use, while ensuring its confidentiality, availability (including reliability), safety, resilience, possession, authenticity, utility and integrity. Systems or processes should be inherently secure, making them resilient to cyber-attacks in line with National Cyber Security Centre codes of practice.[33]

Where a government department or agency is buying technology, the principle of security is covered in the CDDO Technology Code of Practice. Point 6, *Make things secure*, requires a focus on how data and systems are secured.[34] In relation to data security, it says departments and agencies should follow the National Cyber Security Centre's risk management guidance.[35] As many government systems are cloud-based (in line with the government's *Cloud First Policy*), there is also guidance on cloud security.[36]

In the context of the built and managed environment, the *TIP Roadmap to 2030* requires clients to:

> "...follow the sensitivity assessment process set out in Clause 4 of ISO 19650-5 to determine whether to implement a security-minded approach. Where a security-minded approach is required, to develop and implement this following the requirements set out in ISO 19650-5 clauses 5 to 9."

[32] Concept of public good defined in National Infrastructure Commission (2018) *Data for the Public Good*, p.11. 2
[33] See IET/National Cyber Security Centre, *Code of Practice for Cyber Security and Safety in Engineering*, and *Code of Practice: Cyber Security in the Built Environment*
[34] CDDO Technology Code of Practice, Point 6: Make things secure.
[35] National Cyber Security Centre, *Risk management guidance*
[36] CDDO Technology Code of Practice, Point 5: Use cloud first. Related guidance includes the National Cyber Security Centre's *Cloud security guidance*.

4.2.1 What the security principle means for technology providers

The security of information requires a risk-based holistic approach addressing people, process, physical and technical security aspects in response to a documented risk assessment.

Advice on these security aspects is available on the NCSC and CPNI websites;[37] the latter includes resources relating to the *Security-Minded approach to Digital Engineering* including ISO 19650-5:2020.[38]

Technology providers should ensure that their products or services help contracting authorities and their suppliers to maintain necessary security of information. Throughout the lifecycle of asset-related information, technologies should also support management of user access and rights (including by technology providers' employees): preventing unauthorised access, use, disclosure, modification or destruction of information. Where technology providers provide information management services to a contracting authority or supplier, they should also guard against disruption or non-availability of the services.

[37] National Cyber Security Centre - https://www.ncsc.gov.uk/. Centre for Protection of National Infrastructure - https://www.cpni.gov.uk/
[38] Centre for Protection of National Infrastructure, *Security-Minded approach to Digital Engineering* (November 2021).

4.2.2 Related technical requirements

a. **Security certification** – Where technology providers are hosting information on behalf of contracting authorities or suppliers, they should hold appropriate information security management system certifications. In the UK, this should include UK Cyber Essentials Plus and ISO 27001.

b. **Authorisation** – When hosting online systems, technology providers should take appropriate precautions to ensure that individual user access (including users in the technology provider's organisation) has been correctly authorised by an official representative of the customer. Having established their users' identities, methods for future authentication (c, below) can then be followed.[39]

c. **Authentication** – All access to an information management system should be managed through strictly managed authenticated user or machine access service accounts (for example: organisation, framework, project, role, group and user account profiles). Where appropriate, authentication may extend beyond password protection and involve multi-factor authentication, OAuth-enabled single sign-on, FIDO2 cryptographic authentication, or magic links and one-time passwords.[40] An exception would be for access to data covered by an open data licence (eg: Open Government Licence, Creative Commons' Attribution 4.0 licence) enabling its free use, reuse, re-publication and re-distribution.

d. **Users rights/permissions management** – When hosting online systems, technology providers should also provide tools to enable implementation and ongoing management of user access permissions, and fulfilment of any data protection obligations relating to users' personal data, including for marketing purposes.

e. **Access: UI** – User interface access to an information management system should be configurable and based on user, organisation, framework group and role.

f. **API security** – *See 3.2 b), above.*

g. **Information segregation/federation** – *See 4.1.2 j), above.*

[39] See also Centre for Protection of National Infrastructure, *Personnel & People Security* (August 2021).
[40] National Cyber Security Centre, *Authentication methods: choosing the right type* (September 2022).

4.3 Information ownership

The asset owner-operator should procure and specify in contracts that it retains ownership and secures unrestricted direct control over its asset data for as long as required to satisfy asset lifecycle, portfolio or organisational information requirements.

The *TIP Roadmap to 2030* 'Information Management Mandate' tells clients:

> "...the information it procures and holds is an important **asset** with **value**, that is critical to undertaking and optimising the operations, maintenance and disposal of the asset; and [clients should] apply the same level of governance and rigour to the maintenance of its information, to ensure that it provides ongoing value and benefits to the client organisation. This will include the ability to share and exploit information, and also make information available for regulatory purposes."[41] *(emphasis added)*

In addition to the value of asset-related information for operational purposes, it will have value to an organisation as a 'knowledge asset'. Published by BEIS, the Government Office for Technology Transfer and HM Treasury, *The Rose Book: guidance on knowledge asset management in government* (2021) highlights that knowledge assets, including the information an organisation holds, are critical to the effective operation of any organisation, including in the public sector. "Moreover, they are growing in importance, as the role of technology and data in public service delivery increases, and as the government delivers more through partners, where an understanding of the ownership of the underpinning knowledge assets is vital to continued success."[42]

The Rose Book is focused on UK government departments, agencies and public bodies, all of whom generate knowledge assets. Successful strategic management of knowledge assets involves their identification, protection and exploitation to deliver potential social, economic and financial outcomes.[43] It also requires that organisations retain direct control of their data assets to protect against failure of any third party data stewards. *The Rose Book* says strategic management of knowledge assets allows organisations to:

- identify their assets and use them fully to meet the organisation's needs
- save resources by avoiding duplication in the acquisition or creation of knowledge assets
- recognise and reward their staff for innovative work

[41] Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. Annex B: The Information Management Mandate. .
[42] BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, ss 1.4, 1.5 and 1.7.
[43] BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 1.14 (see also HM Treasury (2019), *Managing Public Money*), and s 2.3.
[44] BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 3.2.
[45] BEIS, GOTT, HM Treasury (December 2021), *The Rose Book: guidance on knowledge asset management in government*, s 4.8.

- better protect and enforce their IP (intellectual property)
- lower the risk of infringing the IP of others
- prove their rights in the event of a contractual or IP dispute
- capitalise on opportunities for income generation from knowledge assets, or to deliver wider social and economic benefits
- derive value from underutilised knowledge assets in accordance with principles of *Managing Public Money*
- fulfil financial, record keeping and accountability obligations.[44]

Asset owner-operators' full ownership of their data often includes valuable intellectual property. *The Rose Book* highlights that knowledge assets are often a significant feature of public sector procurements, including infrastructure projects such as roads and rail programmes, giving rise to a range of IP rights (patents, designs, copyright, and databases).[45]

Note: information ownership and value (*see 4.4, below*) are particularly closely connected – asset owner-operators can only recognise and exploit the value of information if they own it.

4.3.1 What the data ownership principle means for technology providers

Technology providers should ensure that their products or services help asset owner-operators to assert and secure unrestricted ownership and control of their asset-related information.

While technology product or services may support information exchanges, they do not entitle the technology provider to any share in ownership of that information. Where technology providers deliver information management services to a contracting authority or supplier, they have an information 'stewardship' role for the duration of their service agreement. As such, they should not seek to restrict or withhold access to information (in the event of a dispute, for example), nor – unless expressly permitted by the asset owner-operator – should they seek to share information with other parties, or use the information to develop new products or services.

4.3.2 Related technical requirements

a. **Ownership and licensing** – Ownership of all containers added into an information management system, metadata and any extracted data, should not rest with the technology provider and access should not be withheld pending resolution of a dispute.[46]

b. **Data residency/sovereignty** – Technology providers should be aware of relevant CDDO-recommended advice,[47] and the data hosting requirements of asset owner-operators.

c. **Data exploitation** – Outside of uses explicitly permitted by the asset owner-operator in product or service licence agreements (or unless otherwise expressly permitted), asset-related data held in an information management system should not be used by the technology provider to develop new products, services or other derivative analyses or insights, or be provided to third parties. For the avoidance of doubt, this includes use of data (even if anonymised and/or aggregated with other data) for machine learning or artificial intelligence purposes, unless it forms part of the service provided to the owner-operator.

d. **Information transfer (returnability)** – When contracted to provide long-term information management services to an asset owner-operator, it should be a contractual requirement that the technology provider should expedite the efficient and timely transfer of all information to the owner, or to its nominated supplier, upon termination of the contract (to the extent that such information had not already been transferred during the contract).

e. **Non-retention** – The technology provider should not seek to retain a copy of any information beyond the termination of an information management services contract (and subject to any agreed requirements relating to service providers' warranties in respect of built asset or infrastructure design, other legal requirements or in relation to professional indemnity insurance obligations). This relates to any information exchanged, managed and stored in the system and any data delivered, extracted or transposed in the system under stewardship by the technology provider. Again, this should be an agreed contractual provision.

[46] In Trant Engineering Limited v Mott MacDonald Ltd [2017] EHWC 2061 (TCC), the Court granted an interim injunction allowing access to a building information model on the basis that access should not be denied by the professional consultant whilst a dispute between the parties about the existence of the contract between them was being resolved.

[47] Central Digital and Data Office, *Cloud guide for the public sector* (February 2021) cites: Information Commissioner's Office guidance on adequacy, and on data protection and the international transfer of data, and NCSC cloud security guidance

4.4 Information value

Information an asset owner-operator procures and holds should itself be regarded as an important asset with intrinsic long-term value. Information should be created, exchanged, (re)used and updated so that it can maximise value (and minimise depreciation) for the owner-operator. The value of information should be enhanced through appropriate sharing, collaboration and exploitation.

Ownership of asset-related information is closely related to how an organisation might recognise and exploit the value of the information it holds. As previously mentioned, the *TIP Roadmap to 2030* tells clients: "...the information it procures and holds is an important asset with value"[48] and *The Rose Book guidance* (see 4.3 above) underlines how that information might be identified, protected and exploited by an organisation to deliver potential social, economic and financial outcomes. There is also an additional opportunity to maximise value during the delivery phase of built or managed assets, in the creation of asset information.

The Rose Book specifically mentions the need to minimise the cost of capturing and processing information, talking of opportunities to "save resources by avoiding duplication in the acquisition or creation of knowledge assets".

Any system or service should, as far as possible, reduce friction in the processes of acquiring, managing and delivering required information and maintaining its value and provenance.

Efficient development of knowledge assets is not possible if planning, design and construction information deliverables cannot be easily exchanged and reused between the software applications used by different organisations or disciplines. For example, imperfect or unreliable export/import processes, or the re-creation of the same information in different proprietary formats, is inefficient. 'Lean construction' processes, by contrast, streamline value-adding activities; they look to enable access to the right information in the right format by the right person at the right time and on their chosen device. This eliminates wasteful processes – for example, initial creation and/or correction of defective information, delivering too much information (too early), waiting for delayed information, additional processing/translation of information, needless dissemination and/or duplication of information, etc. Appropriate agreed lean construction processes should be recorded in the contractual agreement between the parties to facilitate this approach.

[48] Infrastructure and Projects Authority, *Transforming Infrastructure Performance: Roadmap to 2030*, September 2021. Annex B: The Information Management Mandate.

4.4.1 What the value principle means for technology providers

This principle applies to the initial creation and management of valuable information deliverables, to the long-term maintenance of valuable information, and to the potential future exploitation of knowledge assets to create additional value.

First, technology providers should ensure that their products or services are able to help contracting authorities and their suppliers to maximise the value of the information deliverables that users create and exchange. In particular, this means providing technologies that help users to add value to information (ie: to enhance or improve information – avoiding needless recreation or duplication of information, production of unnecessary information, or other wasteful activities; note, appropriate user training may be required so that the products or services are used efficiently and effectively). Software which supports open standards (see 3 interoperability, above) can help users avoid time-consuming export/import or translation processes.

Second, particularly where technology providers deliver long-term information management 'stewardship' services to an asset owner-operator, the technologies should support users in maintaining the value of that information. This includes preventing unauthorised access, use, disclosure, modification or destruction of that information (see 4.2 security, above), while also enabling authorised users to update asset-related information as necessary so that it remains accurate and current. In the case of provision of software as a service, technology providers should implement processes to enable the asset-related information to be curated over its lifecycle, including the provision of appropriate and proportionate measures to ensure the security of the information.

Third, technology providers should be able to support organisations that wish to collaborate by sharing, publishing or federating data.

4.4.2 Related technical requirements

a. **Open standard formats and schemas** – *See 3.2 a) above.*

b. **APIs (application programming interfaces)** – *See 3.2 b), above.*

c. **Information segregation/federation** – *See 4.1.2 j) above.*

d. **Security** – *See 4.2.1 and 4.2.2 above*

4.5 Competition

Information practices should enable fair competition – between the technology providers whose tools enable the creation, exchange and management of information, and amongst users of the tools (for example, supply chain businesses involved in planning, design, delivery, operation, repair and maintenance, and management of assets).

Many software applications create outputs which need to be in a format that can be consistently managed by the software. However, this often means that created content is stored in proprietary formats that software providers may try to keep secret. Consequently, as the information's author, a user or their employer may own the intellectual rights to the information (copyright), but they cannot retrieve it except by using a version of the proprietary software used to produce the file or data. This has two consequences. First, the business becomes dependent upon the vendor's software ('vendor lock-in'), compounded by high switching costs. Second, it cannot then exchange that information with people using competing software, potentially causing contractual issues.[49] Inter-organisation information-sharing therefore requires other businesses to buy the same proprietary software.

This deepens industry dependence upon the proprietary software. It also hampers fair competition between supply chain businesses (proprietary software use may be a condition of appointment, for example) and adds costs for end-users of information (asset owner-operators, may need to purchase the proprietary software in order to access the files or data documenting their assets).

As mentioned *(3 above)*, the need for interoperability to avoid vendor lock-in is covered in government guidance including the *Digital, Data and Technology Playbook* and CDDO Technology Code of Practice. Discussing API technical and data standards, the *Playbook* says:

> "Interoperable data is ...important for a healthy and competitive market. Data which is not interoperable can give incumbent suppliers a competitive advantage when re-procuring and may result in vendor-lock into a specific piece of technology, or supplier software. By allowing equal access to government IT contracts for open source and proprietary software providers, we will create a level playing field, drive competition and incentivise suppliers to co-operate and innovate."[50]

[49] Centre of Construction Law and Dispute Resolution, King's College London (2016), *Enabling BIM Through Procurement and Contracts* (p.48): "31 [out of 40] interviewees stated that interoperability is currently an issue and, at present, not dealt with very well.... 18 interviewees expressed concern as to the export/import of data to and from an IFC platform."

[50] Cabinet Office, *Digital, Data and Technology Playbook*, March 2022, p.61.

[51] CDDO Technology Code of Practice, Point 4: Make use of open standards. The technology section of the Government Service Manual reiterates "Using open standards means you can: ...share data between services and systems more easily [and] avoid getting 'locked in' to a specific piece of technology or supplier".

[52] European Commission, *Competition Policy for the digital era: final report* (2019), and *Data Act* (2022).

[53] Department for Digital, Culture, Media & Sport / Department for Business, Energy & Industrial Strategy, *A new pro-competition regime for digital markets*, July 2021.

The CDDO Technology Code of Practice Point 4, *Make use of open standards*, urges use of open standards as it "increases interoperability and means you ...increase compatibility with a range of stakeholders [and] avoid vendor lock-in".[51] In recent years, the growing importance of interoperability and of open approaches to information sharing have been reflected at both international and national policy levels. Interoperability has been discussed in the context of EU competition policy,[52] and in the context of digital markets. In July 2021, two UK Government departments (DCMS and BEIS) consulted on proposals for a code of conduct for digital firms identified as having strategic market status to support three objectives put forward by the Competition and Markets Authority (Fair Trading, Open Choices and Trust and Transparency). The proposed principles under Open Choices included "c) to take reasonable steps to support interoperability with third party technologies where not doing so would have an adverse effect on customers" (p.31).[53]

4.5.1 What the competition principle means for technology providers

As stated in 3 above, technology providers should ensure that their products or services support non-proprietary exchanges of information between contracting authorities and their suppliers, and between suppliers.

While information will often be initially created and developed using proprietary software or services, when a supplier is contracted to exchange information with a contracting authority or other supplier, that information should be deliverable in a non-proprietary form based on open standards, allowing access and reuse of that information in other software or services.

Technology providers should discourage contracting authorities from mandating use of a proprietary product (or version of that product), or mandating a single proprietary environment – such practices are not good practice, and compromise information sustainability and sound ESG (environmental, social and governance) practices. A contracting authority's information requirements should stipulate the delivery of contracted information outputs in open, non-proprietary forms.

4.5.2 Related technical requirements

a. ***Open standard formats and schemas*** *– See 3.2 a) above.*
b. ***APIs (application programming interfaces)*** *– See 3.2 b), above.*
c. ***Backward compatibility*** *– See 4.1.2 i) above.*
d. ***Information segregation/federation*** *– See 4.1.2 j) above*

By stressing interoperability and setting five underpinning principles that should be adopted by information technology providers, this CoP highlights their critical role in helping asset owner-operators and their supply chains to manage contractual information exchanges.

This first edition sets key foundations and indicates likely future steps intended to further improve good information management practices. The core aim of this CoP is to help UK government and industry respond to new economic, environmental and social pressures by helping the delivery of valuable data, and to build sustainable foundations for future technological opportunities.

Acknowledgements

Discussion and drafting of the first version of *Delivering Valuable Data: An Interoperability Code of Practice for Technologies in the Built and Managed Environment* was a project managed by the GIIG, funded by the Department for Business, Energy and Industrial Strategy, now the Department for Business and Trade.

In May 2023, the GIIG invited expressions of interest from individuals to join a working group to produce the Code. The core working group comprised 16 people (four from asset owner-operator organisations, four from supply chain businesses, and eight from technology providers to the built and managed environment), plus the lead for the GIIG's work on technologies and openness.

- David Bailey – *NHS*
- Bill Davis – *Ministry of Justice*
- John Egan – *BIMLauncher*
- Jo Harris – *Sodexo*
- Andrew Krebs – *SWECO*
- Simon MacArthur – *DocuPing*
- Tom Oulton – *RLB*
- Patrick Owen – *Tideway*
- Fran Parkins – *Ministry of Justice*
- Bruno Postle – *BlenderBIM*
- Jack Seakins – *JLL Smart Systems*
- Marek Suchocki – *Autodesk*
- Paul Surin – *IBM*
- Phil Thompson – *NG Bailey*
- Ben Wallbank – *Trimble*
- Andy Ward – *xBIM*
- Paul Wilkinson – *GIIG (chair)*

The working group had eight full meetings (July 2022 to February 2023) plus interim progress and theme group meetings. GIIG members Louise Dobson, Simon Lewis, Fiona Moore and Nicola Pearson attended meetings of the working group as non-voting members/observers.

The inputs of dozens of contributors to the consultation process in January and February 2023 is also acknowledged.

GIIG

Delivering Valuable Data: An Interoperability Code of Practice for Technologies in the Built and Managed Environment

Version 1.0 | April 2023