HM Government

Information Principles

December 2011, Version 1.0

Table of Contents

Why This Document Is Important

Information is, more than ever, essential to the delivery of public services.

"*Managing information effectively and appropriately is essential to the delivery of secure, seamless and efficient operational services. It provides the basis for informed decision making and the platform upon which performance can be measured. Modern, knowledge-based service delivery underpinned by effective information architecture and open standards will support government to build more transparent, trusted and efficient information exchange processes. The Government will develop an information strategy that is supported by an architecture framework which will underpin the design of government's new information systems*".

Government ICT Strategy (March 2011)

Information is needed to inform policy development and make evidence based decisions, as well as to ensure accountability to parliament and the public. At an operational level, information can be used to drive efficiency and service improvement - enhancing public services, whilst at the same time reducing waste and improving value for money.

"*we will ensure that the datasets government collects are open and accessible in order to support individuals to make informed choices about the services they use*."

Open Public Services White Paper (July 2011)

Furthermore, there is increasingly a drive towards using information to transform public services through transparency and openness, thus enabling innovation and empowering individuals to choose and influence services.

There is however also potential for significant harm to result from information being exposed or misused. It therefore needs to be protected from loss, unauthorised access, and inappropriate use

"*As we go forward, we need to continue to look to find ways of delivering services which meet the needs of the modern citizen whilst taking proportionate and measured steps to manage the risk of deliberate or negligent action which might lead to the compromise of personal information*."

Protecting Information in Government (January 2010)

Given the importance of information to the public sector, there is therefore clearly a need for it to be consistently and effectively managed, protected and exploited. This document therefore presents, for the first time, an overarching set of Information Principles for the UK public sector. The content described here forms a key element of the overarching Government ICT Blueprint. This blueprint is developed and managed using Enterprise Architecture based governance practices, which require that clearly defined principles are established and complied with.

These principles are intended to express timeless truths to which all public sector organisations can subscribe - but also to provide, as a consequence, concrete implications for implementation. The principles are intended be bold and challenging and to set direction. They are not however intended to be directives, and it is for each organisation to consider the principles and to set the extent of their own ambition - interpreting the implications in the light of their own unique organisational context.

The principles provide high-level guidance and therefore their scope is intentionally broad. They apply to all information that is created, collected, held, used, shared, transformed, published or processed by a UK public sector organisation. They apply to both structured and unstructured information, and to information at all stages of its lifecycle[1]. It is again for each organisation to interpret the precise implications in the light of their own unique organisational context and information usage.

As a result, the aim is to enable organisations across the public sector to become increasingly aligned in their use and management of information, drawing their own local strategy and practices from a common set of principles and best-practices.

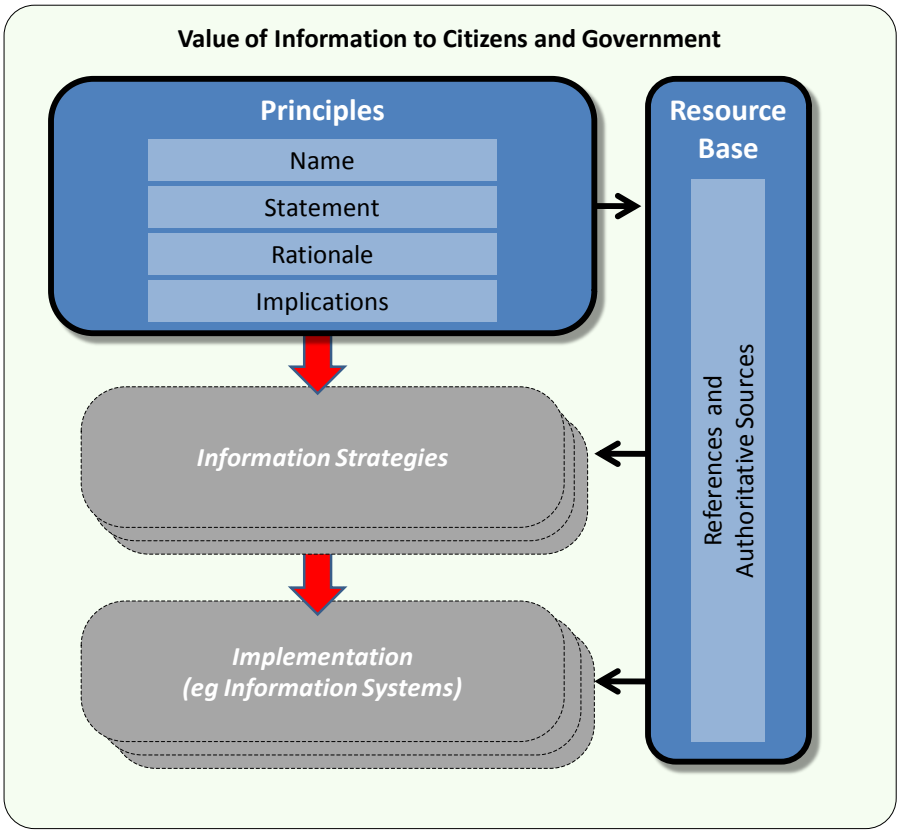
[1] For example, some frameworks make a distinction between Data, Information, and Knowledge – with increasing value, interpretation and insight being added at each stage. This is useful and these definitions are considered further in the Resource Base. However in this document, for brevity, the word “information” is used throughout.

How to Use This Document

This document is intended to be of interest and relevance to a wide readership.

However it is specifically aimed at those responsible for creating Information Strategy for a UK Public Sector organisation. The purpose of the principles is to provide guidance to assist Information Strategies in aligning around a common set of themes and best practices. This helps to provide consistency for an outsider in "reading across" the Information Strategies of each organisation. More importantly it also helps to drive through a coherent approach to realising the value of information for the UK Public Sector as a whole.

The diagram below shows how this works:



- **Value of Information to Citizens and Government**

  The principles are fundamentally based on realising the value of information for the UK Public Sector. Drivers therefore include topics such as those discussed in the previous chapter - for example efficiency, service improvement, citizen choice, value for money, and innovation.

- **Principles**

  Each principle consists of the following parts:

  - ***Name*** – a brief, memorable title
  - ***Statement*** – a more descriptive explanation of what the principle is about
  - ***Rationale*** – explaining why the principle is important
  - ***Implications*** – highlighting concrete implications which arise from subscribing to the principle.

  The implications are particularly important as they provide a checklist of topic areas which an Information Strategy aligned with the principles would be expected to cover[2]. Each implication is supported by further text (in italics) which gives suggestions and examples of what this might include.

- **Resource-Base**

  The principles are supported by a companion Resource Base. This lists extensive references and authoritative sources relating to each principle. The Resource Base thus provides important further assistance for implementation of the principles.

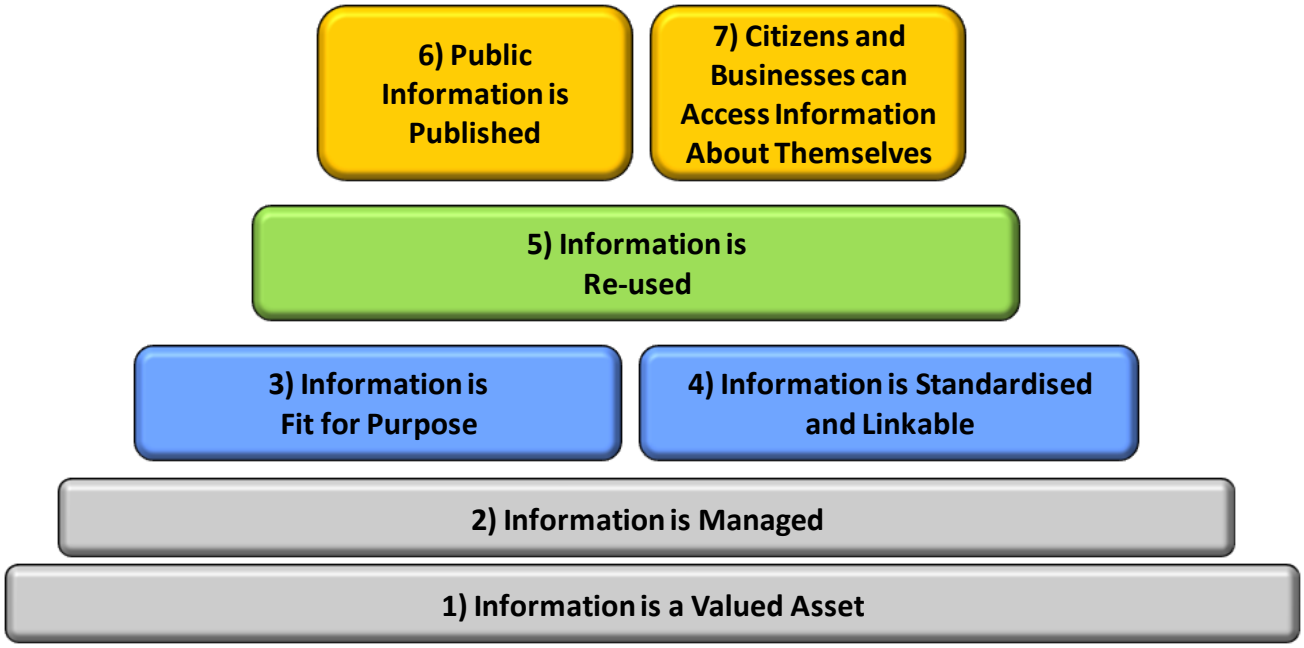
  The resource based can be found at:
  http://www.nationalarchives.gov.uk/information-principles

The remainder of this document describes the principles themselves.

- The next chapter gives a brief overview of the principles as a set, explaining how they form a logical hierarchy.
- Then there is a chapter per principle, explaining each principle in detail.
- Finally, an appendix provides a quick-reference checklist of each principle and its implications.

[2] It is of course likely that in many cases the Information Strategy itself would provide only an overview, and might reference out to more detailed supporting documentation (policies, process definitions etc) for the details

Principles Overview



Seven principles have been identified. They build naturally into a hierarchy, as depicted in the diagram above.

The hierarchy is important as the principles build on what has gone before. For example it is unlikely that information can be re-used unless it is also valued, managed, fit for purpose, and standardised.

The first two principles provide a foundation as the basis on which all other uses depend. It is important that information is valued as an asset and managed, protected, and exploited throughout its lifecycle. It needs to be governed with regard to regulation, and based on a consistent approach to risk assessment. Organisational roles and responsibilities should be in place, and skills and capabilities developed.

The next two principles help to unlock the value inherent in information. Information need not be perfect, but it does need to be fit for purpose - both in terms of its technical format and also in terms of conforming to well-defined quality characteristics. It also becomes more valuable when it is made available in standardised forms and is linkable to other information and authoritative sources.

With these pre-requisites in place the principle of re-use can be achieved. Re-use both avoids wasteful duplication, and provides the means to extract value in new and innovative ways.

The top layer builds on all of the layers below, providing transparency by opening up access to information. Two principles are highlighted – the publishing of public information, and ensuring that citizens and businesses have access to information about themselves.

Principle 1 - Information is a Valued Asset

Statement

Information is an asset which is fundamental to the efficient and effective delivery of public services. This principle emphasises the importance of an organisation understanding the information that it uses and valuing that information in business terms. It draws the parallel with other organisational assets (eg buildings, machinery, people, money) - highlighting the need for information to be understood, recorded, valued, protected and exploited like any other organisational asset.

Information has a purpose, and in order to fully understand its value it is necessary to understand the purposes for which information is created and managed. This includes consideration of both the original purpose for which information is collected and also, as far as can be anticipated, any subsequent downstream uses.

Rationale

The valuing of information as an asset provides the foundation on which all other principles depend.

Knowing what information exists, along with an assessment of its usage and value, is a prereqisite for all other information management practices. It is also a prerequisite for appropriately protecting and fully utilising and exploiting the information. With regard to exploitation, there is increasingly an expectation that public sector information assets will be put to work and exploited for the public benefit.

Implications for Information Strategy

There is a declaration from the organisation to establish the importance of information to the business
The approach is defined for consistently identifying, categorising and cataloguing Information Assets and their purpose • *Both structured and unstructured information assets need to be*

considered[3]*.*

- *Consideration needs to be given both to information which is directly "owned" by the organisation, and also to information that is handled - ie there will be information that is owned and managed elsewhere but which is relied upon to deliver services*
- *It should include cataloguing the known purposes to which information is put*
- *Consideration needs to be given to the appropriate level of detail to capture*
- *The approach should include a process for periodic review and update, as the purpose, usage and value of information may change over time.*

A framework for assessing and recording the value of information assets is established

- *This should consider value to:*
  - *The originating organisation itself*
  - *The wider public sector and providers of public sector services*
  - *Other users - for example citizens, businesses, academia, or not-for-profit organisations*
- *The approach to recording the value of information assets should be established. (For example, this might include linkage to both information management practices, and also to wider corporate approaches for asset management and accounting)*

[3] The concept of an "Information Asset Register" may be helpful in cataloguing information assets, see Resource Base for more details. However the intent of this principle is simply to state that a list of information assets is needed. Some implementations of Information Asset Registers are more constrained (for example holding structured datasets only). In practice therefore the approach may need to explain how this will be supplemented with other lists / catalogue(s) in order to provide a complete view of all an organisation's structured and unstructured information assets.

Principle 2 - Information is Managed

Statement

Information Assets are stored, managed, protected and exploited in a manner commensurate with their value.

This requires consideration of the lifecycle through which all information moves – for example from identification of need, creation, quality assurance, maintenance, re-use, and ultimately to archiving or destruction once it has ceased to have a business use. A range of information management best-practices need to be applied throughout the lifecycle - for example to ensure appropriate availability and integrity, to avoid exposure and loss, and to ensure continuity across technology upgrades. It is particularly important that personal data is adequately protected.

Furthermore information needs to be governed as it moves through its lifecycle ensuring, for example, clarity as to who is responsible for it (ie an identifiable owner), and compliance with all relevant legislation and regulation. The consistent assessment and ownership of information risk is another important consideration.

In order to apply these best-practices it is necessary that a suitable organisational culture be established, and that those processing information are professionally qualified and skilled to do so. This principle therefore also includes the processes, roles, responsibilities, training, and organisational structure and culture needed to ensure the effective and efficient use of information in enabling an organisation to achieve its goals.

Rationale

Modern ways of working are increasingly knowledge-based, and mature information management practices are essential to support this. Information also needs to be well managed as it may need to be used to provide evidence demonstrating accountability to elected representatives and the public.

In terms of protecting information, poor information management and governance practices expose the public sector to unnecessary risk. For example, the public sector is a custodian for large volumes of personal information and the public have a right to expect this to be kept safe. Poor practices may also lead to inconsistencies which may subsequently incur costs and/or reputational loss. It is particularly important when considering new technologies to make sure that the risks are appropriately balanced against the opportunities and benefits.

In terms of exploiting information, poor information management and governance practices may result in an overly risk averse approach which hinders information sharing and re-use.

The need therefore is for appropriate policies and frameworks which allow information to be shared and re-used for legitimate purposes - whilst at the same time ensuring that information is protected so that legal obligations are met and so that only those who need to have access may do so.

Implications for Information Strategy

A framework for managing information through the different stages of its lifecycle is established • *This should include establishment of a set of lifecycle stages, and identification of best-practices for information management at each stage.* • *Examples could include records management practices such as establishment of a corporate repository, retention schedules, and procedures for disposal / archiving of information that no longer meets a business need.*
The approach to digital continuity is defined • *This should consider planning based on the alignment between the lifecycle for technology and the lifecycle for the information it manages.* • *Also the approach for selecting a format and medium to store valuable information.*
A framework for information risk assessment and risk management is established • *This should include defining the approach to protecting information consistent with its value, ownership, and source in order to ensure integrity, confidentiality and availability.* • *Also including identification of key transfers of information between process, systems or organisations* • *It is recommended that information management is included in an organisation's Risk Register*
The approach to ensuring legal and regulatory compliance is defined • *Processes are defined for identifying and ensuring compliance with relevant laws and regulations for each information asset.* • *Including, for example, policies and training to ensure that personal information is handled appropriately*
The approach to Information Governance is defined • *Including consideration of:*   ○ *Roles and responsibilities (eg SIRO, Information Asset Owners, DRO)*

○ *Controls and assurance (eg defined IA policies, approach and compliance on protecting information)* ○ *Organisational structures and accountability (eg Information Governance Board)*
A skills framework and / or maturity model is established to develop organisational capabilities and culture for information management

Principle 3 - Information is Fit for Purpose

Statement

Having considered the purpose of information in Principle 1, it is important to ensure that information is of sufficient quality to meet the purpose for which it is intended. This includes both its primary purpose and also any additional secondary purposes to which it might also be put. Furthermore, in an environment where information is widely reused and published, it may not always be possible for the originator to foresee all potential downstream uses. Therefore information quality needs to be communicated consistently to those that may wish to re-use it, so that they can objectively judge for themselves if it is suitable.

The aspects of quality include factors such as accuracy, validity, reliability, timeliness, relevance, and completeness[4]. The actual quality of information should also be regularly monitored to ensure that it at least meets the levels that have been assessed as necessary for its purpose.

A further aspect of this principle is considering alignment between information and its supporting technical platform and format. For example, if information were to be needed for online statistical analysis then it would be inappropriate for it to be locked up in a proprietary legacy system, or stored offline on back-up tapes, or only available in an unstructured PDF format.

This principle doesn't require information to be perfect, only that it is of sufficient quality for the intended use, and that its quality characteristics are advertised with the source itself.

Rationale

An understanding of the quality characteristics of information is essential to its appropriate use, and is particularly important when judging its suitability for re-use to meet new purposes. Similarly, it is important that information is supported by a technical platform that is capable of delivering the intended usages.

Drawing conclusions based on information of insufficient quality is clearly inappropriate. However equally undesirable is withholding information that, while imperfect, could still provide value and be fit for some purposes.

[4] Audit Commission: "Improving information to support decision making: standards for better quality data" 2007. Note that other data quality classification schemes are also available, see Resource Base for more details.

Implications for Information Strategy

An approach is defined to determining the right quality of information to meet its purpose • *This would typically build on the catalogue of Information Assets and their usage identified under Principle 1, identifying the quality characteristics required in each case* • *Note that the emphasis is on "right quality" rather than necessarily on "top quality". Information just needs to be good enough for the purpose for which it is used*
A consistent approach is established to describing, recording, and communicating information quality • *For example based on defining quality characteristics and metrics* • *A mechanism should be defined for quality characteristics of information to be communicated when information is published*
Processes and governance are established to monitor and assure information quality • *This is necessary to ensure that information is of adequate quality for its intended use* • *Should include prioritising areas for quality improvement*
An approach is defined to recording the relationship between information and its supporting technology platform and format • *Should include assessing this technology platform and format for suitability against the information's purpose*

Principle 4 - Information is Standardised and Linkable

Statement

The opportunities for exploiting information greatly increase when it is made available in standardised and linkable forms.

Standardisation is relevant both to structured information (eg in terms of dataset definitions), and also to unstructured information (eg in terms of the metadata tags applied to documents). Some value is unlocked by standardising information within an organisation, however there is even more value in making information available using widely accepted Open Standards.

Standardisation needs to be considered on a number of levels including:

- Standardisation of format (eg date is represented in format yyyy-mm-dd)
- Standardisation of content (eg forename, surname, address etc)
- Standardisation of concepts (eg patient, offender, learner, claimant, driver – are all roles that a person can take)

Further value can be unlocked when information is made available in a form that can be linked.

The linking of documents provides a familiar example of this – with references and citations allowing the reader to draw in a wealth of associated documents providing further information. (This idea is the basis of the world-wide-web).

However a similar concept can also be applied to structured data - based on an understanding of the relationships between items, and the use of consistent identifiers to reference authoritative sources. (This idea is the basis of the “semantic web”). For example, tagging spending information with an authoritative code for the organisation involved would allow it to be unambiguously linked with both details of the organisation itself, and with other information held elsewhere about that same organisation (eg service satisfaction measures).

Note that, as always, this principle builds on what has gone before. So Principle 2 establishes the need for appropriate governance over information linking - for example with regard to any privacy constraints. And Principle 3 highlights the need to take into consideration the quality characteristics of information which is being linked.

Rationale

The use of standards, in particular widely accepted Open Standards, unlocks value by enabling others to understand and re-use information by providing it in a consistent and comparable format and by freeing it from proprietary lock-in.

Furthermore, the value of information can be enhanced when it is linked to other information. When information is linked then users can explore and discover new information that is useful to their needs. The benefit from linking information grows exponentially as more information is linked, and more links are established between information.

Implications for Information Strategy

There is a commitment to Open Standards • *A commitment of intent to adopt Open Standards where these exist and to promote new standards where they should exist.*
Corporate standards are established for the organisation • *An information standards catalogue is established, with preference being given to widely accepted open standards* • *An appropriate set of models is established for documenting the meaning of the organisation's information and relationships between items (eg ontology, data models)* • *A corporate Data Dictionary is established, including common vocabulary and definitions* • *A consistent approach to applying metadata to documents is established*

A framework for linking information is established
• *Aspects to consider include:*
  ○ *Unambiguous identification of items (eg using authoritative reference data, or URIs)*
  ○ *Classifying items and the relationships between them.*
  ○ *Linking of items (eg potentially using the open standard web mechanisms governed by the W3C)*
• *Consideration should be given to both internal linkages to other information sources within the organisation, and also to external linkages to other information sources across government.*

A pragmatic approach for migrating to standardised, linkable data is established

- *An approach is established for new systems (eg a commitment for all new systems to be built using linkable/API-accessible open-standards-based methods).*
- *An approach is established for existing systems (eg identification of priority areas, cost/benefits, and strategy for consolidation, referencing, and linkability of information in legacy systems. Also approaches to mapping where necessary between data formats in existing internal systems, and externally exposed Open Standards)*

Principle 5 - Information is Re-used

Statement

The value of information can be multiplied by re-use. This requires a change of mindset – to think outside of traditional silos and proactively look for opportunities to re-use.

Aspects of re-use include:

- Internal re-use - making sure that full value is gained from using information for its primary purpose, and furthermore identifying secondary uses to which it can be put. For example, operational data can sometimes be re-used to support performance improvement or research.
- External re-use – sharing information with others across organisational boundaries, whether within the public sector, or more generally with private businesses and citizens
- Master data - a further aspect of re-use consists of ensuring only a single authoritative source for business information exists (eg an authoritative list of organisation codes) - nominated, maintained and promoted as such.

Re-use involves considering what information an organisation can make available to others, but it also involves looking at what others have on offer, and how an organisation might itself re-use this external information.

Whilst this principle strongly encourages re-use, it is important to appreciate that re-use does require a careful risk-based judgement to be made with regard to exploiting vs protecting information, as well as consideration to the costs and benefits involved, and any rights or other commercial considerations.

However note that even information which appears initially unsuitable may often be reformatted for re-use. For example, operational information that identifies individuals can be ‘anonymised’ or aggregated and then be of wider value. Also, in cases where the partner organisation is known beforehand, then concerns can sometimes be mitigated by means of negotiation, joint-working, and data sharing agreements.

This principle again builds on what has gone before - as information re-use will not to be achieved to any significant extent unless information is effectively managed, strong governance processes are in place to manage the regulatory[5] and risk-based implications of re-use, the information’s quality characteristics and fitness for purpose are defined, and it is made available in standardised and linkable formats.

[5] For example the 2nd data protection principle states that personal data shall not be further processed in a manner incompatible with the purpose for which it was obtained.

Rationale

Re-use of information presents opportunities for cost savings and efficiencies. There is a cost and burden to collecting information and, once collected, opportunities should be sought to extract additional value by appropriate and innovative secondary uses. In addition there may be opportunities for the re-use of information to lead to consequent cost savings from further consolidation within the systems portfolio.

More broadly, a "joined up" approach to the sharing of information across the public sector to deliver public services and to meet public task responsibilities is becoming increasingly important and expected. Information may also need to be re-used to demonstrate accountability and as evidence to Parliament to audit and to Public Inquiry (eg Bloody Sunday Inquiry, Iraq Inquiry).

Finally, re-use avoids the problem of multiple sources of information within an organisation competing to be the authoritative source, or worse, the use of sources under the false assumption of their authority.

Implications for Information Strategy

Opportunities to proactively offer re-use opportunities are identified

- *For example, an assessment is made of the reuse potential of each information asset (e.g. considering costs, benefits, and priorities)*

Mechanisms are established to understand and, where possible, overcome the constraints on re-use

- *Linkage is established with the management and governance processes covered under Principle 2 - in order to assess the balance between protecting vs exploiting information, reach decisions on any risks involved, and to put in place additional mitigations where appropriate*
- *Constraints on re-use are periodically reviewed, to make sure that they remain relevant and valid*
- *Mechanisms are identified to extract and transform information, where necessary, into a format that is more suitable for re-use. Aspects of this include:*
    - *Presentation – to maximise usefulness, and to help ensure information is correctly interpreted*
    - *Derivation – to add value to the information for –reuse*
    - *De-sensitising – to enable otherwise sensitive information to be released. (Specific techniques might include anonymisation, pseudonymisation, aggregation, redaction, etc)*
- *Partner organisations are identified, and the establishment of appropriate*

information sharing agreements considered

An approach is established for promoting information that can be reused
• *For example by publishing a list, both internally and / or externally*[6]
• *The terms by which information is offered for re-use are published which may include:*
  ○ *defined legal gateways*
  ○ *consents*
  ○ *commercial and licensing terms*[7]
  ○ *governance undertakings*

An approach is established to discovering information that can be reused • *An approach to search and discovery is established (eg search tools, use of internal and external catalogues to discover reusable information assets)* • *A review process is defined which considers re-use possibilities before approving new data collections ("COUNT" principle - Collect once use numerous times)*
The approach to managing Reference / Master data is established • *Including the use of external sources where these are authoritative*

[6] Note that configuration management may need to be considered as part of this publication approach – to ensure that there is clarity as the version being made available and the impact of any subsequent changes

[7] Note that the default position should be for information to be made available free of charge - for example under the Open Government License

Principle 6 - Public Information is Published

Statement

Public information includes the objective, factual, non-personal information on which public services run and are assessed, and on which policy decisions are based, or which is collected or generated in the course of public service delivery[8]. Public information should be published, unless there are overriding reasons not to.

Crucially, this principle goes beyond the minimum requirements imposed by legislation[9]. It advocates a proactive approach to publication of information – ie to presenting, formatting and promoting information in useful formats for wider consumption, without it needing to be specifically requested or mandated in legislation.

Note that publishing information to the public also requires consideration of the practical channels by which this will actually be achieved. This includes the establishment of internal publication processes, the use of publication hubs (eg data.gov.uk), as well as potentially relationships with 3rd party "information intermediaries"

Clearly the desire to publish information does need to be balanced against constraints which may prevent this. Exclusions would include, for example, personal information, information which can compromise privacy, commercially and legally privileged information, and information that is required to maintain security. However note that in some cases information which appears initially unsuitable may be reformatted for publication, as discussed under Principle 5.

Rationale

Publishing public information provides benefits to government, communities, and citizens such as[10]:

- Making government more accountable and approachable - enabling citizens to hold the government to account.

[8] See working definition of "Public Data" http://data.gov.uk/blog/new-public-sector-transparency-board-and-public-data-transparency-principles. Note that, as per the introduction to this document, the word "information" is used in a broad sense in this document. In practice the decision about what to publish will need to be considered for each step in the lifecycle as "raw data" is enriched and becomes "information" and then "knowledge". For example there may be cases where it is appropriate to publish the raw data, but not necessarily the results of analysis based upon this.

[9] For example Freedom of Information Act (FOI) and Environmental Information Regulations (EIR)

[10] Extracts taken from "Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office" by Kieron O'Hara

- Creating better value for money by providing an insight into how money is spent, encouraging departments to improve controls on spending and reduce their costs.
- Stimulating growth by enabling businesses to develop innovative information-based products and applications using public data.
- Reforming public services by:
    - Providing choice and improving public sector outcomes, by giving citizens the information they need to make informed decisions about the public services they use, and giving providers the incentives they need to improve the quality of their services and to develop new innovative services.
    - Opening up public sector contracts, giving companies, social enterprises, charities and employee-owned cooperatives the opportunity to compete to offer high quality services by providing access to public sector contract and procurement information.

Furthermore, publication of information also has the potential to reduce the costs and risks of information management. This is because, once published, a self-service approach to accessing the information is possible and also because the risk of accidental exposure then becomes irrelevant.

Implications for Information Strategy

A framework is in place for responding to legal obligations regarding public access to information • *For example: Freedom of Information Act, Environmental Information Regulations*
Going beyond the legal obligations, a framework is in place for proactively categorising information in terms of its relevance and suitability for publication • *A publishing schedule is established, for example prioritising information assets where there is a publicly expressed interest, as well as specific consideration of information relating to satisfaction and public experience.* • *A process is established for periodic review of the publishing schedule, to ensure that it remains relevant and up-to-date.* • *Processes are defined to consider new requests for information publication* • *Publication of both structured datasets and unstructured information (eg documents) is considered*
Channels and processes for publishing information are established • *Plans for publishing relevant information are outlined.*

- *Publication interfaces, websites, or feeds are identified (eg data.gov.uk)*
- *Consideration given to equality issues (eg access for those without internet access)*
- *An approach is established for the potential use of any external 3rd parties ("information intermediaries") to transform and add value to the information.*
- *Governance processes and policies are defined, particularly for the management of continual release of the same dataset (e.g. monthly).*

A pragmatic migration approach for publishing data is established

- *An approach is established for new systems (eg a commitment for them to be built with an automated or semi-automated publication route built into them for everything that can be released (e.g. finance systems), or aggregation to defined levels (e.g. management information tracking systems)).*
- *An approach is established for existing systems (eg identification of priority areas, cost/benefits, and strategy for extracting information from legacy systems)*

Principle 7 - Citizens and Businesses Can Access Information About Themselves

Statement

Citizens and Businesses should be able to access information about themselves, along with an explanation of how it is used. This may be either on request or, preferably, by making it available by default. In effect, such information should be considered as belonging to the citizen, although entrusted to the care of a public body.

Note that this principle goes beyond the minimum requirements imposed by legislation[11]. It advocates a proactive approach to allowing citizens to access information about themselves, without it necessarily needing to be specifically requested or mandated in legislation. This might be achieved, for example, by making it securely available online[12]. Consideration needs to be given to both viewing and, where appropriate, to performing transactions such as updates (for example to correct inaccuracies).

Clearly the desire to make information available does need to be balanced against constraints which may prevent this. Exclusions would include, for example, legally privileged information, and information that is required to maintain security[13].

Rationale

Providing citizens and businesses with access to information about themselves, when taken in conjunction with the public information published under Principle 6, completes the picture in terms of the information which is relevant to inform a citizen's choices and interactions with the public sector.

> "*We believe that when people have the power to make decisions and exercise choices to meet their own needs, the value of public funds can be greater than when the state makes decisions for them.*"
>
> **Open Public Services, White Paper, June 2011**

On a day-to-day level there is the opportunity for both reduced costs as well as improved service. For example, at its most basic, providing citizens with access to information about

[11] For example Data Protection Act (DPA)

[12] Note that consideration does clearly need to be given to access and inclusivity - bearing in mind, for example, those with disabilities, or with limited access to ICT

[13] Again, further details of relevant exclusions can be found in legislation such as the Data Protection Act

themselves by default negates the need for specific processes and systems for responding to Subject Access Requests. However the opportunity extends far beyond this, in terms of enabling automated self-service access to a wide range of public sector services.

> *"Easy-to-use, trusted and flexible online transactional services, such as student loans or Jobseeker's Allowance, reduce the bureaucratic and time burden on citizens. Therefore, the Government will work to make citizen-focused transactional services 'digital by default' "*
>
> **Government ICT Strategy, March 2011**

Implications for Information Strategy

A framework is in place for responding to legal obligations regarding citizens' access to information about themselves and how it has been used • *For example: Data Protection Act and Subject Access Requests*
Going beyond the legal obligations, opportunities are identified to proactively make information about citizens available to them by default • *For example opportunities for read access and/or to request updates via secure online channels* • *Identification of priority services to make available via automated digital self-service*
The approach to discovering information about a person is established • *For example based on consistent person-centric data models and document indexing*
A pragmatic migration approach is established for enabling citizens' to access information about themselves • *An approach is established for new systems (eg to include provision for Subject Access Requests, person-centric identification of information, ability to provide secure online access).* • *An approach is established for existing systems (eg identification of priority areas, cost/benefits, and strategy for providing citizen access to information in legacy systems)* • *The approach is established to authentication of citizen- as an enabler to providing them with access to their own information*

Appendix A – Summary of Principle Implications

This appendix summarises for ease-of-reference the key implications of each principle. Note that it is still important to read the main document section about each principle for further explanation and context.

Principle 1 - Information is a Valued Asset

There is a declaration from the organisation to establish the importance of information to the business
The approach is defined for consistently identifying, categorising and cataloguing Information Assets and their usage
A framework for assessing and recording the value of information assets is established

Principle 2 - Information is Managed

A framework for managing information through the different stages of its lifecycle is established
The approach to digital continuity is defined
A framework for information risk assessment and risk management is established
The approach to ensuring legal and regulatory compliance is defined
The approach to Information Governance is defined
A skills framework and / or maturity model is established to develop organisational capabilities and culture for information management

Principle 3 - Information is Fit for Purpose

An approach is defined to determining the right quality of information to meet its purpose
A consistent approach is established to describing, recording, and communicating information quality

Processes and governance are established to monitor and assure information quality
An approach is defined to recording the relationship between information and its supporting technology platform and format

Principle 4 - Information is Standardised and Linkable

There is a commitment to Open Standards
Corporate standards are established for the organisation
A framework for linking information is established
A pragmatic approach for migrating to standardised, linkable data is established

Principle 5 - Information is Re-used

Opportunities to proactively offer re-use opportunities are identified
Mechanisms are established to understand and, where possible, overcome the constraints on re-use
An approach is established for promoting information that can be reused
An approach is established to discovering information that can be reused
The approach to managing Reference / Master data is established

Principle 6 - Public Information is Published

A framework is in place for responding to legal obligations regarding public access to information
Going beyond the legal obligations, a framework is in place for proactively categorising information in terms of its relevance and suitability for publication
Channels and processes for publishing information are established
A pragmatic migration approach for publishing data is established

Principle 7 - Citizens and Businesses Can Access Information About Themselves

A framework is in place for responding to legal obligations regarding citizens' access to information about themselves and how it has been used
Going beyond the legal obligations, opportunities are identified to proactively make information about citizens available to them by default
The approach to discovering information about a person is established
A pragmatic migration approach is established for enabling citizens' to access information about themselves

Appendix B – History and Contributors

These principles have been endorsed by:

- The CIO Delivery Board
- The CIO Council
- The CTO Council
- The Knowledge Council

The principles in this document are based on earlier work led by Tariq Rashid and Neil Dench within the CTO Council Information Domain. An extensive consultation process was then followed to evolve and refine the principles to the current version. This has included several workshops, plus review via an online survey which was widely circulated to representatives from CIO Council, Information Domain, and Knowledge Council.

Many thanks to all who have contributed, including:

Name	Organisation	Role
A M Cassels	Fera	Information Centre Manager/Agency Record Officer
Alison Thompson	MMO	Director of Corporate Support and Governance
Allan Reese	CEFAS (via DEFRA)	Senior statistician Cefas
Andrew Newman	Defra	Engagement Manager - UK Location Programme
Andrew Wharrad	Defra	Data Architect in Defra
Ben Plouviez	The Scottish Government	Head of KIRM
Colin Hand	Ministry of Justice	Information Architect
David Coker	DfT	Data Protection Officer
David Elder	GCHQ	Information Management
David Roper-Newman	Department for Work and Pensions	Departmental Security Policy and Standards Manager
Des Livings	DCMS	Head of Information Services
Farah Ahmed	Cabinet Office	Head of Right to Data Implementation
Group Captain Q Dixon	MOD CIO	Dep Head Strategy and Plans
Hannah John	Department for Transport	KIM Policy Lead

Name	Organisation	Role
James Forrester	Cabinet Office	Digital Engagement Policy Lead
Jeremy Boss	Audit Commission	CIO (completed with Head of Information - Diane Skinner)
John Adams	DFID	
John Sheridan	The National Archives	
Jonathan Budd	Natural England	Knowledge and Information Strategist
Kerry MacLean	Crown Prosecution Service	Departmental Security Officer
Linda Wishart	Department of Health	Head of Knowledge and Information Management
Mark Merifield	The National Archives	Manager of Records and Information Services - collating this response on behalf of TNA
Mark Reynolds	Department of Health	Director - Information Standards Board
Neil Dench	Department of Health	Architect
Neil Neville	MOD	
Paul Davidson	Sedgemoor District Council and Local eGovernment Standards Body (LeGSB)	Chief Information Officer (SDC) and Director (LeGSB)
Paul Turton	HMRC	Lead Enterprise Architect
Paul Willman	Crown Prosecution Service	Deputy Departmental Records Officer
Roger Smethurst	Cabinet Office	Head of Knowledge and Information Management
Stuart Laidlaw	Cabinet Office	Information Compliance Manager
Toby Anscombe	Ministry of Justice	Information Architecture Manager
Valerie Hope	Defra	Policy officer on the Environmental Information Regulations 2004
William Barker	DCLG	Cross Govt Digital Policy, Strategy & Innovation