Socitm

Harnessing data:

Information management principles *BETA*

BETA version

The content in this section is available in a BETA version and is currently being reviewed.

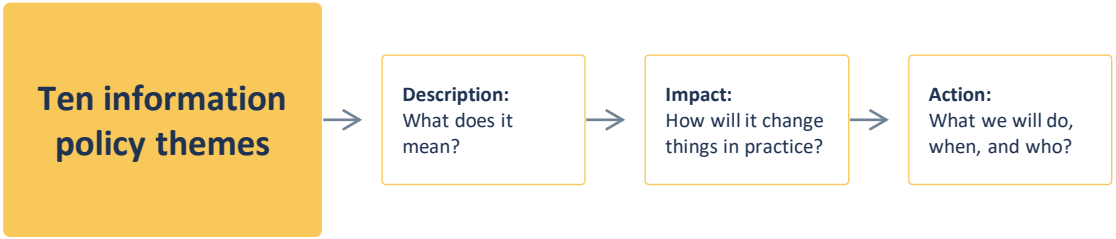
Please send any comments and suggestions, additional resources and/or case studies that may help to improve or update this content to:

martin.ferguson@socitm.net

Information management principles

Policies and principles for information management need to be established. Whilst these will vary to an extent in different public service organisations, there should be commonalities, especially in good information governance, data ethics and standards. But more importantly, they need to form the basis for how the business uses data and information – from front line staff to the executive team and politicians, and the information specialists in IT, audit, legal, finance, social care, data protection, and elsewhere.

Teams across public service organisations need to be trained in and clear on how they will apply information governance and practice in order to maximise the value of information assets safely and responsibly. This includes information used in corporate performance management, democratic processes, partner sharing, legislative compliance, risk management and support of digital and IT strategies. There should be no excuse that “I was not told” or “I did not know” in terms of ethical, safe and appropriate use of information in the public interest.



e.g. Camden Borough Council has a clause in every contract that says access to data is on demand

Information management principles **example descriptions**

Ten information policy themes

Eliminating paper

Information is captured, stored and distributed electronically wherever possible, to keep offices clutter free, to support new ways of working and to reduce costs. Reducing paper reduces information risks (storage, loss, error) and increases information value (sharing, analysis, linking). Paper archives are only for statutory requirements and corporate records management policies and lifecycle management assume electronic capture and storage. Paper use is limited to temporary work action – and then recycled, not stored.

Information skills

Employees are competent in using information appropriately and safely. They understand and abide by policies to ensure data and information are kept safe and handled appropriately, knowing how to report incidents or vulnerabilities. Everyone understands that good data and information husbandry is their responsibility – it is not just for IT service providers to protect the organisation. Digital maturity and information risks from poor practice will be regularly audited and reported (e.g. in controlled 'phishing' tests). Failure to observe good practice (e.g. falling for an external phishing attack) could be a disciplinary offence.

Easy search and retrieval

The organisation recognises that being able to find information is more important than being able to file it (the purpose of filing is retrieval). The key to this is classification, meta-data and referencing. Information is classified, and attributes are assigned, to facilitate search, external sharing, and links to relevant data held by other organisations. This will include all data types – electronic documents, databases, voice, IoT data, video, geographic data and images, across the whole council.

Information efficiency

Common data sets are captured once, as close to the source as possible, and shared as many times as needed. Collect the right data at the right time. This reduces duplication of data sets and of keyed input, increasing consistency, lessening the cost of both input and maintenance. Where related information is derived from different sources it is pooled in a single common dataset and shared to be used many times by different users, for different purposes. Duplication of data capture and storage, especially as a result of resistance to sharing, is avoided, and there are systems and technologies to ensure information quality is tracked and maintained.

Open and shared

Information managed by the organisation as a whole and in departments specifically, is treated as a corporate resource. The culture is 'open' with respect to all data, with a willingness to share information internally and externally, unless there is a compelling and documented reason not to do so. Legislative requirements to share and to keep data safe are widely understood and part of training awareness. Social media, internally and externally, is used effectively to increase collaboration, awareness and openness.

Focus on users

Information systems and websites (internet and intranet) are designed around user needs. This means easy and intuitive access, from anywhere, at any time, using any device (as far as possible). All systems are developed jointly with users (co-design) and accessibility over service delivery efficiency will be prioritised where possible. Rather than disenfranchising or depersonalising, digital delivery will be more accessible to more people, providing a more personal and tailored experience. Customers can log in and see their data and transact, end-to-end, with minimal or no support wherever possible. Aim to capture all customer data required at the first point of contact

Information for management

Management decisions are informed by relevant, accurate, timely and consistent information. This includes democratic processes and reporting to members. Effort is made to identify information needs for decision makers, and to mine and extract the information required to satisfy these needs, using appropriate tools and analysis. Example information sources for management support include geographic, performance, risk, personal and commercial data.

Common standards

Data standards are adopted for all core data sets, especially where these relate to personal data. Key systems (core) for the council, such as email, finance, web, content management, CRM etc., are identified and drive information and data standards across the council. Common systems and processes exist for managing information, including data held in line-of-business systems and the prioritisation of open APIs.

Cyber and privacy

Data and information assets are subject to appropriate safeguards and protections, with a corporate inventory of information assets. The confidentiality, integrity, legality and reliability of information is maintained. Cyber security is reported to the board regularly – including activity, audits and incidents relating to data security, wider corporate information risks, business continuity, and community resilience. Employees, members and suppliers understand their data security responsibilities. Physical security practices ensure no unauthorised access to buildings or equipment that may compromise information systems. The public can be confident that personal or commercially sensitive information is appropriately protected and not misused or abused. All information has a named owner and all staff will ensure appropriate levels of security classification are held against documents and data sets. All systems are rigorously tested, and as far as possible logon access is harmonised across services (e.g. single login method and identity management).

Accurate and timely

Decision making depends on fit-for-purpose information: information that is accurate, complete, relevant, up to date, authorised, set in context, and well presented. The organisation ensures that processes, practices and resources are in place to achieve data quality across its key information assets and to provide analysis and reporting capabilities that support effective information provision and decision making.

Information management principles **example impacts**

Ten information policy themes

Eliminating paper

All forms will be electronic, 'end-to-end' and automated, and paper use will be limited to transient purposes; e.g. recycled at the end of a meeting/project where some paper use is unavoidable but not stored. Office space will be released, filing cabinet use minimised. Printing volumes are monitored by team, project, and individual usage, to identify and address unnecessarily high levels. Fax machines and personal printers are not used except in exceptional cases. Systems enable effective archive and retrieval of electronic data and records, ensuring that statutory duties for storing paper are met, without extending unnecessarily into other areas.

Information skills

Staff and members are inducted and trained in the information management skills relevant to their role. Information skills are explicit in job descriptions, recruitment, and HR policies. This includes when staff responsibilities change in relation to data use. All relevant staff and third parties are kept up to date with records management policies and processes to ensure statutory compliance. IT systems, access methods and support are designed and implemented to make security compliance easy, requiring minimal or no training. Specialist training will nonetheless ensure specialist areas, such as Audit, are effective 'data scientists', able to spot and manage changing systems risk in complex IT architectures as well as data and information quality issues.

Easy search and retrieval

Eliminating paper and ensuring that all information is managed consistently (e.g. formats, metadata etc), increases the value of information and its security. This will help in the management of personal data in particular – its identification and linkage when necessary or appropriate. It can also increase equality of access to electronic services and information for the public, giving users choice in how to access information and reducing access barriers due to age, disability, language or socio-economic grouping. Systems for access, storage and sharing of data and information will be unified across the council as far as possible, to reduce training and support needs of staff and to increase the potential value of data analysis and insight. This will help with corporate performance management, service delivery activity and audit controls.

Information efficiency

Document and record management systems are harmonised, integrated or ideally replaced with one unifying corporate system, as far as possible. All document and electronic records systems have effective version control and appropriate security controls to avoid multiple copies of the same report (for example) with appropriate security access. The IT Strategy mandates the adoption of core systems, rationalising overlapping or unnecessarily fragmented systems to help to generate a single view of data sets (e.g. finance, staff, property, performance, citizen contact data sets). A strategic approach to cloud adoption avoids a fragmented patchwork of cloud services that make data difficult to reuse. Aggregated demographic and performance data is captured once and then shared internally or with partners and the public.

Open and shared

All data is seen as a 'corporate asset', wherever it may be captured or owned locally, and is expected to be shared internally. This means systems should not lock data into proprietary formats, instead using open APIs and formats that make data sharing and extraction easy. Unless there are legal restrictions or other risks of confidentiality, sensitivity or privacy, information is accessible both internally and externally by partners, citizens and businesses. This may mean reducing internal (intranet) use in favour of universal web access for staff and the public, especially for customer contact staff. This in turn will assist customer support teams. The LGA Data Handling Guidance will be adopted in full. 'Blanket' security and confidentiality rules will not be applied to documents or data bases without good reason. Openness is balanced against the risks of inappropriate disclosure, and open data will reduce FOI burdens over time.

Focus on users

As far as possible, systems will allow users (staff, partners, politicians, and the public) to access data and information that they need. Usability testing will be a key part of all systems design and specification, whilst recognising the need for process change to ensure systems reflect working practices to achieve this goal. Specific skills exist in IT in screen design and navigation, and development methods focus on delivering an excellent experience for users. Contact centre and customer service staff have a significant say in how and where systems need to be adapted to reflect the pattern of usage and feedback from customers. Web platforms are developed to embrace transactions and service delivery in their design, not just as information sources or as marketing tools.

Information for management

To support a strong evidence-based decision making culture, the organisation will invest in the tools, techniques and analytical skills required to gather, store, aggregate, analyse, interpret and present information to support strategic and operational decision making. Resources invested are proportionate to the benefits delivered. Performance management and performance reporting are straightforward, with systems designed to collect the right information and pass it to management systems, with a range of presentational formats. This allows community intelligence to be developed as a strategic resource (e.g. for resource allocation, planning, community projects, building capacity, policy development, service delivery and improvement, and wider place-shaping).

Common standards

The systems, processes and standards used for the creation, storage, retrieval and disposal of information are the same across the council, regardless of department or location. Open data (e.g. open and common APIs), personal data and other specific data sets all adopt common formats that avoid duplication, poor data matching or errors. Data standards help to maximise the value of information assets, facilitating information sharing and partnership working. This also provides consistency for users, reducing the cost of systems acquisition, maintenance and support. Legislative requirements relating to information management are widely understood and are applied in the most cost-effective way, again using data standards.

Cyber and privacy

Unauthorised access to and/or modification of information is prevented by managing information with appropriate security practices. Personal data is readily identified and managed in accordance with legislative requirements (e.g. GDPR). Good information practice enables information to be used more widely, safely shared and accessed on personal devices where appropriate to support mobile and flexible working. Audit trails identify who has accessed sensitive data and any changes to data made. Regular penetration testing, data audits and usage pattern tracking spot risks and intrusions early. IT will work towards ISO27000 compliance, whilst PSN (and related) compliance, IT disaster recovery and backup testing are mandated and effective, developed together with corporate business continuity planning and emergency planning. Regular data audits test the effectiveness of IT security practices and are reported to the board. Role based security and associated tools ensure that all access to sensitive data is appropriate, monitored and breaches identified. Access control and identity management systems provide easy yet safe access to data and systems for the public, employees, partners, suppliers and members, reflecting their roles and access rights.

Accurate and timely

Information is only acquired and maintained as required for delivery purposes and to meet corporate aims. When new services are provided, or existing systems changed, priority is given to ensure that data quality is not compromised, information needs are assessed, and common formats are adopted which enable data sets to be linked. Data quality in systems is audited and processed, to correct errors or omissions. This will reduce risks exposed through data testing in upgrades, integration projects or systems replacements.

Data design principles

At a more detailed level than information management principles (which is about data use) there are some simple data design principles which can help to form the foundations for good information use and policies.

Each organisation is different, but here are some examples to act as a guide:

Data Principle:	Description:
Start with the data, not with the technology	Technology is just an enabler, so ensure that you consider your data needs and *then* have a technology plan that can support it, rather than buying clever data capture and reporting technologies without understanding how you're going to use them. Equally, just because there are ways of analysing data and linking data together, doesn't mean you actually want to do that or capture the data in the first place. Decisions about data should be informed by how you are going to use it and the decisions you're intending to take.
Data is the key, not information	Information is the value that you extract from data, but this changes, so don't become fixated on the information and data use. Data is valuable in many ways and data that you capture today for a specific purpose will be used tomorrow in ways that you cannot envisage. Moreover, the quality of information and the way in which it is used and interpreted depends on the quality of the underlying data and its provenance.
Data ethics matters	It is easy to say, and who would disagree? But actually quite hard to ensure high levels of integrity in how data is used in practice. It is worth defining clearly what 'data ethics' actually means for your organisation, and this should encompass the priority for the citizen and the data owner more than the organisation consuming the data on their behalf.
Be clear about data ownership	It is important to have someone taking responsibility for the quality of data sets, how data is used, shared and maintained. At the same time, data must not be locked into service silos by owners or systems– "it's planning data, you can't have it". It can be helpful to think in terms of data custodians rather than owners, after all, data is mostly corporately owned (or should be), or is owned by citizens.
'Data people' matter	In Audit, IT, and in digital teams data skills are essential. But they are also essential for data analysis, risk management, and in how we can safely deploy new technologies such as artificial intelligence. Invest in the necessary data skills across the whole of the organisation, and in particular in prioritising the specialist roles that support data use.
Data can drive process redesign	We often start thinking about the data sets necessary to support a business process. But actually data can define what a process should look like: for example, well-designed data sets, linked together in citizen records, can shine a light on how to design functions better to meet citizen need.
Data formats should be consistent	In the past we have captured similar data in slightly different formats – partly because of different neds and sometimes because the technology required this. Consistency in data formats (such as key identifiers – name, address, asset numbers etc) is fundamental to opening up the possibilities of data and ensuring accuracy and integrity of data sets on which increasingly important decisions are being made.

Master data management

Data governance can help public service organisations to make the most of the data available to them. This includes data asset management and control (who owns data and what are the responsibilities of ownership?), as well as ensuring a good understanding of which data is sensitive and how it should therefore be managed and used. A common approach to data management across the organisation helps to order structured and unstructured data as well as ensuring data quality and authenticity for deriving business insights and intelligence.

Master Data Management is a systematic way to manage, centralise, organise, categorise, localise and to link data typically around a specific topic area (well-being, environmental practice, etc). It can create a single (virtual) repository of data across multiple cloud and on-premise data sources, as well as data held by partners. Its primary function is to increase data value and ensure a move away from the inefficiencies caused by data silos.

> “Master data management involves establishing a common language for customer products and other essential domains as the foundation for analytic efforts. This is more critical today than ever before. Data governance controls are required to ensure consistency in adoption of evolving digital platforms, operating models and even vision.”

Master data management

Effective control of corporate data in this way opens up many possibilities for insight, predicative analyses and practical linked data opportunities:

- Individual data sets suddenly offer new insight and value
- We can see what information is actually available to us previously locked in systems and silos
- We get a single view of data – citizens, property assets, business opportunities
- Service demand drivers are clear to understand, predict and to influence
- We understand the needs and preferences of residents and service users
- Decision making is faster and better, and we become more agile and flexible as a result
- It is easier to spot problems before they arise and to intervene appropriately
- Politicians feel more in control by understanding voters preferences and concerns and it can support democratic processes
- We can begin to tackle cross-service and cross-organisations data challenges
- Its is the only route to solving complex issues – pollution, transport management, troubled families, crime and its causes, health and social care integration, etc.

Additional resources

ODI resources:

- How to create a data inventory guide
- The Data Ecosystem Mapping tool (as part of the Data and Public Services Toolkit)
- Developing a data management plan: a checklist