LBM Information Management Strategy

Contents

1 Introduction
2 Where do we need to be?
3 Design Principles
4 Strategic outcomes
   4.1 The business need
   4.2 Senior Governance
   4.3 How we use our information
   4.4 Data Quality
   4.5 Data Sharing
5 Policy

Appendix 1 What will the future look like – TOM
Appendix 2 Overview of Information Asset Owner Audit and Information Sharing Audit
Appendix 3 Action Plan

1 Introduction

Information is a key asset to the council. Whilst it does not appear on the balance sheet it needs to be used appropriately, protected and, where able, exploited in the same way as other assets. Information enables service delivery, informs decision making and tells us how well we are performing. The council holds vast quantities of information, including personal and sensitive client information and commercially sensitive business information.

The good governance of this information is managed through organisational policies such as the Data Protection Policy and the Information Security Policy and compliance with the Data Protection Act (personal data). The Caldicott Board oversees the management of social care records and the council’s Senior Information Risk Owner (SIRO) oversees the Information Risk Policy and Risk Register. Poor information management can lead to ineffective services, bad decisions, reputational damage and a possible fine, undertaking or enforcement action from the Information Commissioners Office (ICO).

Excellent information management brings numerous benefits to the council and to staff, including improvements in efficiency and effectiveness (through having the right information in the right format at the right time with the right person in the right place),
improved regulatory compliance, preserving the corporate memory and a reduction in storage requirements (both physical and electronic).

The ever changing technology environment impacts on how we use, exploit and protect our information.

Information is one of the nine layers in Merton’s framework for developing Target Operating Models (TOMs). The TOM framework is used to ensure that all services are planning for and shaping their future and that change and transformation takes place in a controlled and disciplined way. The nine constituent layers allow the current and target operations to be systematically mapped and analysed and ensure that there is a proper understanding of how the council works and how it could work differently in the future to deliver strategic objectives. This means each and every service expressly considers its approach to and use of information when planning for the future.

The outcomes of the departmental TOMs will feed in to this strategy, to ensure that the requirements of all of the organisation have been considered and planned for.

This strategy, refreshed in February 2014, draws on this work to ensure that the planned change and transformation in relation to information is supported and coordinated.

The information management strategy will assist Merton in meeting its strategic themes, including those areas of corporate capacity, which will result in improved governance, access to services for residents and customers, value for money services and a well trained and equipped workforce.

The Local Government Association and the ICO have written to all council leaders urging them to take stock of how their council meets its data protection obligations and how they exercise their governance responsibilities. They have provided a checklist of questions for councils to consider how well they are doing and also advise councils to think about how they oversee such an important part of the council’s work. During 2014, the ICO will have to take a view as to whether there has been sufficient improvement in local government's data protection compliance. If not, the ICO will have no option but to seek further powers to undertake compulsory data protection audits of local authorities. Taking action to make certain that the senior leaders (both political and officer) of the council are fully engaged in data protection and information management more widely will go a long way to ensure that this key risk area is properly managed – to the benefit not just of the council’s stretched finances but of the corporate reputation as well.

The ICO has also recently stated in their own consultation document ‘Looking ahead, staying ahead’ that one of their main challenges is ‘We’re in the growth business. Information rights are of growing importance in the public mind, prompted by developments in technology, business and public policy. That means we’re busier than ever’ and ‘Information is the currency of democracy’. 
2 Where do we need to be?

These outcomes have been developed following a review of the council’s current position and industry best practice, and represent the Information layer TOM focusing on where the council needs to be.

- **Knowing what information we have and what is needed** – this is to ensure the information we have is managed correctly and efficiently and information that we require to improve service delivery and value for money is acquired.
- **Knowing who uses the information and who it is shared with** – this is to ensure that the correct people are accessing the information, information is being held securely so there is no unauthorised access and, that where applicable information is shared to assist partnership working.
- **Knowing the quality of our information** – this is to ensure that the council’s information is of the highest quality so that good quality decisions are made using accurate and timely information.
- **Setting open data as a default information approach** – so the public are able to find the information that they require and the council can become more transparent and accountable.

3 Design Principles

The design principles support the Information Management strategy and will drive forward how the council manages it information.

- Clear and appropriate accountability for all Information Assets
- COUNT – Collect Once Use Numerous Times – subject to DPA requirements
- Timely accurate data available to customers
- Establish primary and secondary datasets and sources
- Data shared safely and securely
- Data quality standards met
- Information as an asset – subject to relevant legislation
- Open data by default

4 Strategic Outcomes

4.1 The business need

**Flexible working and information access**

The council is moving to more flexible and mobile working arrangements for staff. This means that information assets need to be stored and managed in a way so that they can be accessible at multiple locations, at times they are needed, can be easily shared and worked upon by a number of people in real time and are kept secure, safe and usable for all business purposes.

To achieve this, a rationalisation of systems needs to take place, with mobile access and appropriate security as key drivers for this. The adoption of a council wide electronic
Information governance requirements will also need to be part of the move to flexible and mobile working to ensure staff are aware of both best practices for managing information and the increased need for security of information. This will be in the form of policies and guidance, staff awareness campaigns and specific training as required.

**Actions**

- Rationalisation of the number of systems in use in the council.
- Information governance issues to be considered as part of the move to flexible and mobile working.
- Undertake a staff awareness campaign and a programme of specific Information governance training.

**Improving the customer experience and decision making**

The council needs to continuously improve its services and offer residents increased value for money. Information is central to service improvement. At a basic level, the effective management of information can improve productivity and working processes; over and above this, good decisions about improvement and targeting of service delivery are informed by having access to high quality information. This information will need to include our customers’ needs, how our services are performing, how our resources are being used to deliver services, how services are best commissioned for effective resource use and to meet needs, and what our customers think about and how they experience our services.

To achieve this, effective information management needs to be part of all process redesign to ensure that adequate and accurate information is always available. Data quality needs to improve council wide to ensure that timely performance and management information is available to assist good quality decision making. An effective and central intelligence resource needs to be maintained to ensure that information about customers, including their needs, what they value and their experiences, is available to assist in service improvements.

Information management also needs to be a key consideration of all future partnership working to ensure efficient and effective working arrangements are in place. This will include decisions about ownership of information, agreements and guidance around the information lifecycle and appropriate and lawful information sharing with adequate security in place.
**Actions**

Effective central intelligence source to be maintained about customers.

Information sharing and management agreements to be in place for all partnership working.

**Storage and duplication**

As the council rationalises its office accommodation and the amount of electronic information held continues to increase, the effective management of information is essential for staff to be able to access the quality information they require, when and where they require it. Storage options need to be considered to ensure that they are appropriate, fit for purpose and reduced where possible. Reduction of duplicate information held by the council will enable the remaining information to be more easily managed.

The use of the Information Asset Owner (IAO) role will assist with assigning responsibility for information assets, and a rationalisation of systems will help with reduction of duplication. A council wide EDRMS will also assist with reducing duplication through multiple access capabilities, scanned images to reduce paper requirements, and robust security controls to ensure sensitive information is protected.

Other areas of work that are required are effective records management controls to manage information lifecycles to be an essential consideration for all system procurement. The need for a council wide approach to physical record storage options, for both short and long term options and to take into account both individual service area needs and business drivers, should be produced. Staff also need more awareness of their responsibilities in managing information and the tools for them to do this, through awareness campaigns and Intranet resources.

**Actions**

A council wide approach to storage options (physical and electronic) to ensure their appropriateness and that they meet business requirements.

**Records management**

Records management is the systematic control of records, throughout their lifecycle in order to meet operational business needs, statutory and fiscal requirements and user expectations. This includes all records regardless of format and structure. Records need to be managed from their initial creation to their eventual disposal. Effective management of council information allows fast, accurate and reliable access to records. It ensures the timely destruction of redundant information, in compliance with the DPA, and the identification and protection of key information resources, including the historical record of the borough.
A council wide classification scheme, based on the Local Government Classification Scheme, will be introduced in order to assist with easy saving and retrieval of information. Records will be saved according to agreed naming conventions and with standard metadata and data labelling, to aid searching and sharing of information. These standards will apply to all of the council’s structured data, with the aim that solutions will be found to bring unstructured data management up to these standards. New record formats, including social media, will also need solutions for their management in line with records management standards.

Retention of information is also vital. All records will be subject to a retention schedule and will be destroyed in line with this, unless there is good reason which will be decided on a case by case basis and the decision will be recorded. The retention schedule will meet business, legal and regulatory requirements. Where possible retention will be made as automatic as possible to ease the process and ensure good practice is achieved and this will be facilitated with the EDRMS.

It is essential that the council dispose of all information in a secure manner. The council’s retention and destruction procedures will ensure compliance for physical information records. The secure destruction of information, both physical and electronic, as part of the wider disposal of storage facilities and ICT equipment, must comply with the council’s agreed destruction procedures and in line with the IT strategy.

**Actions**

A council wide classification scheme to be set up.

Standard naming conventions, metadata and data labelling to be put in place.

Systematic retention to be in place for all records.

Adherence to the council retention schedule.

### 4.2 Senior Governance

**Senior Information Risk Owner**

Responsibility for the improvement of the management of information and the risks around this need to be owned at a sufficiently high level in the council to ensure it is given the level of importance required. This role is the council’s Senior Information Risk Owner (SIRO), and the position is held by the Director of Corporate Services. The SIRO also oversees the council’s risk management strategy and corporate risk log so information risks will be given the appropriate priority.

Responsibility for data quality, information security, records management, legal compliance, information sharing and publication will be delegated to Information Asset Owners (IAOs). The Information Governance function will be responsible for providing advice, policy and process, identifying standards, measuring compliance, improving performance through training and identifying and mitigating associated risk.
The Information Governance function will also ensure all new uses of information and sharing of information is appropriate and complies with DPA requirements and that all procurement or enhancement of information systems considers information governance issues.

To ensure these requirements are met an Information Governance Board should be set up, to be chaired by the SIRO, and made up of representative IAOs, IT and Information Governance specialists. It will promote awareness, review security and confidentiality breaches and provide a yearly report to the SIRO. A separate board will ensure compliance with Caldicott and joint working across Health, Social Care and the Children’s Trust.

**Action**

Information Governance Board to be set up, chaired by the SIRO and attended by representative IAOs and IT and Information Governance specialists.
Information Risk Policy to be updated.

**Information Asset Owners**

A cultural change is required in the management of information assets, including recognising *information as an asset*, as well as people, and *clear and appropriate accountability for all Information Assets*. The council needs greater transparency and clarity about the ownership of information assets and that information assets are kept suitably safe according to sensitivity. Due to the sheer amount of information held, the Information Governance function cannot be responsible for every information asset; instead responsibility needs to reside with the business using the information to ensure service requirements are met.

IAOs will be designated for each of the council’s information assets. IAOs will be responsible for the data quality of the information, information sharing by ensuring it is both secure and legal, appropriate information security, records management in line with the retention schedule, legal compliance and the appropriate publication of their information. They will be expected to work towards agreed corporate standards based on levels of risk and strategic importance of their data, as well as the capabilities of the system they manage.

Standard information contract clauses should be in place for the procurement of all new systems and any service delivery contract.

IAOs responsibility will cover both electronic and non-electronic information assets, including paper files and micro-fiche and photograph stores.

Owners of unstructured data systems used across the council, such as the email system, will only have overall responsibility for legal compliance and security.
IAOs will work with the Information Governance function to develop local records management procedures detailing how corporate policies are complied with at system level. IAOs will be responsible for ensuring that all users of their systems are aware of their responsibilities regarding the information they process.

Regular audits of information systems will show the level of compliance against corporate standards, and allow managers to make judgements about the quality of the information that informs their decisions.

IAOs will also need to be aware of the future requirements of their information asset, including changes in legislation or reporting requirements and what information they will need to collect or access, so the council is able to plan for and respond to these needs in a timely manner. This will include the need for IT input, audit assistance, training requirements and information governance or legal advice.

**Action**

Information Asset Owner to be in place for every information asset in the council.
Training to be provided on Information Asset Owner responsibilities.
Develop standard information contract clauses.

**Training**

Information security training is currently delivered through computer based learning, whilst DPA awareness training is provided via departmental inductions and other targeted training. There is also a library of guidance, procedures and useful information on the Intranet for staff to use.

Training should be delivered based on the likely needs of the individual and team and the information that they handle. A suite of computer based learning modules needs to be created that are more council specific. A number of these modules should be undertaken in the initial days of an individual’s employment, and subsequent, more advanced modules completed depending on the information processed by individual staff. These modules need to include handling information requests, information security, information sharing and privacy needs.

Staff will be required to carry out on-line information security training at least every 18 months to ensure their knowledge is up to date. Lists of staff who fail to complete this training in a timely manner will be reported to DMTs, who will be expected to follow up each case to ensure compliance.

**Action**

Information security and governance training to be geared to individual and team needs and enforced.
4.3 How we use our information

Data Protection

The Data Protection Act (DPA) controls the use of personal data. It requires that all uses, intentional or otherwise, of personal data follow these principles:

- Collection and use must be fair and lawful,
- Collection and use must be for specified purposes,
- Data must be adequate, relevant and not excessive for the purpose,
- Data must be accurate and up to date,
- Data must not be held longer than necessary,
- Individuals may access, correct and restrict use of their data,
- Data must be held and handled securely, and
- Data must be protected when sent, or stored, overseas, with increased protection outside of the EEA.

The DPA has implications for most of the themes in this strategy, and needs to be at the forefront of any information decisions, as the ICO is able to audit public bodies and can impose fines of up to £500,000 for breaches of the DPA. From April to December 2013, 180 local authority data breaches were reported to the ICO, representing 15% of the total number reported. Five local authorities were fined ranging from £70k to £150k.

Action

All offsite storage solutions, including Cloud storage, must be DPA compliant.

Privacy

Customers should be able to share and maintain their information with the council via self-service access with confidence that the council will use their information effectively and lawfully. They will expect the council to be transparent in the way their information is used and ensure that their privacy is respected at all times, especially when using the COUNT principle – collect once use numerous times. Above all they will expect their information to be kept securely. The council is working to establish how best to roll out COUNT, ensuring compliance with the DPA and also managing the public expectation of how they expect the council to look after and share their information.

As part of the Customer Contact programme the ability for customers to share and maintain their own information via self-service needs to be explored. This information can then be used to update the council wide EDRMS or other systems, to ensure that services always use up to date information and the customer only needs to provide this information once.

Information security remains important and best practice for security in the public sector will be adopted. IAOs will also have responsibility for the security to the information held...
in their systems, and information about staff access and their access permissions needs to be collated and held.

Reviews of all privacy notices and information sharing agreements need to take place regularly to ensure that customers know who their data is being shared with. The council’s website will also clearly state how customers can complain if they feel that their privacy has been breached, and how to find out who their information is being shared with and how to stop this sharing if required (though consequences to their service delivery will also be explained if sharing is disallowed with certain organisations).

**Actions**

- Implement COUNT principle, ensuring compliance with the DPA.
- Regular reviews of all privacy notices and information sharing agreements.
- Clear guidance for the public on the council’s website about how to complain if they feel their privacy has been breached or want to find out more about information sharing.

### 4.4 Data quality

In order to ensure effective decisions are made, the quality of the information held by the council needs to be trusted. Information needs to be kept up to date in a timely manner, and regularly checked for quality to ensure that decisions are made using the right information and that *timely and accurate data is available to customers*. With increased information sharing between organisations it is even more important that good quality, accurate and up to date data is shared.

A reduction in information systems and the use of a council wide EDRMS will help improve data quality across the council and ensure that information is held in a common standard format. Standard formats will be developed for the council for commonly held data like addresses and dates of birth and these will facilitate the combining of and sharing of data. Future information system procurements need to ensure that information is held in a council-wide common standard format, to ensure information can, where appropriate, be easily shared between systems.

IAOs will be responsible for ensuring *data quality standards are met* by ensuring the accuracy of their information and metadata, the timeliness of updates to their data and quality audits of their information. This will ensure data that is shared, published or used to respond to an information request can be trusted to be accurate.

The Information Governance team will set data quality standards and provide guidance and advice on achieving good quality data.
4.5 Data sharing

Local authorities operate in an increasingly complex environment with multi-service responses, multi-dimensional partnerships, integrating services across organisations, increasing customer expectations and new ways of working all pointing to the need to collaborate and share data safely and securely. In order to support a learning organisation there is an increasing need to capture and maintain operational knowledge, share this with other staff and make it available to support succession planning and sustainable solutions.

In order to achieve this, a council wide EDRMS should be adopted that is easily accessible across the organisation, providing both collaborative working and the secure management of sensitive information in shared environments. The EDRMS will also support the management of email, which is essential for evidence of previous business decisions and enabling knowledge sharing. Good search and retrieval functions are vital.

Information security management and standards, including secure email facilities are vital for data sharing, and the council must ensure best practice with their security tools, including protective marking of information and secure data transfer. An improved approach to internal publication of information also needs to be put in place; this will ensure that publishable information is available to all, break down information silos and reduce duplication and repetition of work already carried out.

Information sharing agreements need to be written and kept up to date for all data sharing, and held centrally. Privacy impact assessments need to be undertaken for all projects, new systems and significant changes to working practices. Publishing these documents routinely will enable the public to see that the council are meeting their requirements under the DPA, considering carefully the risks inherent in sharing information, and keeping service users more informed about how their data is being used. IAOs will be responsible for ensuring this happens, using corporate templates and guidance.

Actions

Implement a council wide EDRMS.

Publish all information sharing agreements and privacy impact assessments.

Open data
There has been a tremendous shift in the public sector towards transparency, and alongside the publication scheme requirements of the Freedom of Information Act, the Department for Communities and Local Government have a code of recommended practice on data transparency. The requirement to publish will become law in spring 2014. Alongside this, customers are expecting to be able to access more services and carry out more transactions online.

Transparency brings many benefits including, helping democracy by enabling people to get information they need to be engaged in the political process, driving public service reform and helping to generate economic growth.

In order to meet these requirements, the council needs to move to a culture of open data by default, where publication of information on the Internet should occur unless this would breach confidentiality, the DPA, or the conduct of business. Teams and IAOs should continuously review their information to see if any further data can be published, including establishing primary and secondary datasets and sources. Ease of use of the Internet and its searching tools are key to ensuring an open data culture is effective. The Internet also needs to be managed to ensure out of date information is removed, and therefore optimising search results to enable people to find information most relevant to their needs as quickly and efficiently as possible.

Where possible all published data should be in an open source format to allow individuals and organisations to combine data sets to produce new information products. This will allow businesses, academics and the wider community to unlock the potential of the information collated by the public sector. By publishing information we are enabling others to suggest or provide innovative services to our residents and also supporting the growth of a knowledge economy.

The access of more services and completion of more transactions need to be made available on line. The Customer Contact programme will enable most of this to take place, but needs to consider the information governance and security issues that will need to be managed to make this work.

**Actions**

As much up to date information to be published on the Internet / Intranet in a timely manner.

Regular scheduled removal of out of date information by IAOs on the Internet / Intranet to ensure ease of access and searching.

Open source formats to be used for published data where possible.

**Information requests**

The council is receiving an increasing number of information requests as public authorities are required to become more accountable and transparent in their decision making and as the public understand more about their rights under information laws.
An open data culture will assist with a small percentage of these information requests; however as requests become more detailed and specific, improved processes need to be put in place to assist the council in responding to these requests. These processes will describe roles and responsibilities, contain templates for ease of response, and checklists and flowcharts to ensure the correct response is sent out in a timely fashion, first time. Reviews of information requests that do not meet the customer’s expectation are both costly and time consuming.

A rationalisation of information systems, a council wide EDRMS and improved physical storage options, will enable the information for requests to be gathered more efficiently and effectively and more timely and improved responses to be achieved.

This will also enable subject access requests for personal data to be responded to more accurately and efficiently and in line with statutory timescales.

**Action**

Improved guidance and process to ensure information requests are responded to correctly and in a timely fashion.

**5 Policy**

This strategy document is supported by the Information Governance Policy and the Information Security Policy. These policies are supported by procedures and guidance covering:

- Retention and disposal of information
- Information sharing
- Rights of access to information
- Secure handling of information

These documents are available at [http://Intranet/information-governance](http://Intranet/information-governance)