Gloucestershire County Council

Information & Data Management Strategy

2019-2024

Getting the most from our information

information management & security

Work Smarter

Working more effectively

Gloucestershire County Council

Information & Data Management Strategy 2019-2024

Getting the most from our information

Information and data are critical to every part of the council's business. Managing and using it correctly, protecting it appropriately and making it available to both stakeholders and the public enables the council to fulfil its objectives, deliver improved services and increase our standing with the public.

Key themes in the previous strategy were around information governance and information asset ownership and responsibilities. Due to considerable efforts in every part of the council, we have achieved major improvements in the way we handle information and have an established network of Information Asset Owners. It is essential that we sustain our focus on these important elements of information management so that the public can maintain trust and confidence in the way we operate. We have also explored the potential of improving our data analytics to achieve greater value from our data in informing decisions and achieving better outcomes for our communities and undertaken a proof of concept to develop essential insights.

But, increasing demands for the right to government information and data means the relationship between the citizen and the public sector is changing. We are also entering a new digital era which will transform the way that public services are used and delivered. In responding to these challenges, the council is embracing a move towards greater openness and maximising the value of information to help facilitate closer collaboration and digital services.

This refreshed information & data strategy sets out our approach to managing our information to achieve the right balance between making information more widely available to the public, whilst ensuring that adequate protection is in place.

Why do we need a strategy?

Information comes in many forms – policy documents, research papers, minutes, statistics, operational data, case files, personal data – and is held in a variety of printed and electronic formats. Across the council we use this information in our daily working lives as we work to achieve our objectives – whether it be delivering services, formulating policy, managing projects, holding meetings or managing staff.

Many services are now delivered in partnership or are commissioned from third parties. This requires additional safeguards when managing our information: we need to ensure that information ownership is clear, the right people have appropriate access to the right information and it is handled correctly throughout its lifecycle.

The council is transforming the way we do business with our customers and increasing provision of digital services. The council's digital vision is to digitally connect our community, county and council and put the power in people's hands by being an insight driven organisation. Improved digital options so that more customers choose to do business with us online, through increased self service, leading to more end-to-end transactions, more mobile working, automated workflow and virtual contact by staff; good information management is an essential part of this.

Evidence-based decision making requires good quality, relevant and timely information and data interrogation tools to support service delivery and the planning of future services, performance monitoring and nationally required returns.

We need flexible and agile teams across the council; staff need secure access to the information they need, at any time, from anywhere.

To encourage a 'One council' approach and reduce silo working, records must be regarded as corporate rather than personal assets. This means a change of culture from relying on information held by individuals in their personal P: drives and email stores, as well as manual storage units.

In addition, there is now more external scrutiny of how councils manage their information, through enhanced data protection legislation, and a move towards greater openness and transparency around the information that we hold.

To maximise the potential benefit from our information, we need to manage it effectively, re-use it where we can, share it appropriately and ensure that it is adequately protected. Past experience has shown us that this does not always happen – information that is not managed properly may be lost, shared with the wrong people or not found at all.

Poor data quality and failure to manage information appropriately can lead to:

- Less value for money in terms of service delivery
- Additional costs of recreating or recovering lost information, and storing or digitising information we don't need
- Poor outcomes for customers, poor decision making, difficulty, delays or additional costs in providing on-going services
- Poor external inspection outcomes
- Loss of access to information (e.g. security incidents or systems unavailable) impacting rights and freedoms
- Penalties and fines.

This strategy sets out Gloucestershire County Council's approach to improving the way the council creates, uses, manages, shares and protects information to achieve the council's objectives and effective partnership working. The strategy is aligned with our Digital and ICT strategies in order to provide a comprehensive and integrated approach.

Benefits

When information and data is well managed it brings a number of benefits both to citizens, staff and the council:

Citizens

- Your information is accurate, reliable and accessible
- Your transactions with the council and its commissioned service providers and partners will be processed promptly
- You will be confident that your information is protected and handled appropriately
- You will know what information we hold, how we use it and whom it is shared with
- Services are delivered more efficiently and cost effectively
- Decisions that affect you are more transparent
- You can participate more in decision making
- You can engage and collaborate with us in achieving our aims
- You can hold us to account

Staff

- You can find the information you need quickly and easily
- You know what your responsibilities are, what to keep and what to dispose of
- You can work more efficiently
- You can make the best use of resources, re-using information that you and colleages create rather than reinventing the wheel
- You can work more collaboratively, making best use of skills and knowledge
- You know what can be shared and with whom
- You know what information needs to be protected and what should be made available to the public
- You can provide assurance that risks are being managed and that you are complying with your responsibilities and legal requirements

The council

- We can provide more effective services and help control costs
- We can be more transparent
- We can keep information protected and secure
- Our information risks and likelihood of associated fines of up to £17million are reduced
- Our customer experience is improved
- We build trust in the quality of our information both for staff and the public
- Our decisions and policies are better informed
- We can comply with legislation
- We can share our corporate memory with future generations
- We can meet expectations of how we will manage information
- Through the role of Information Asset Owners (IAOs), we are aware of our information holdings

Legal & Regulatory Requirements

There is a complex legal framework under which we must manage the information we are responsible for. This includes, but is not limited to, the following:

- General Data Protection Regulations 2016
- Data Protection Act 2018
- Digital Economy Act 2017
- Freedom of Information Act 2000
- Environmental Information Regulations 2005
- Re-use of Public Sector Information Regulations 2015
- INSPIRE Regulations, 2009
- Local Government Acts 1972, 1985, 1988 and 1992
- Public Records Acts 1958 and 1967
- Regulation of Investigatory Powers Act 2016
- Copyright, Designs and Patents Act 1988 and the Copyright and Rights in Databases Regulations 1997

In addition, there are many information requirements specified in legislation governing the provision of services to children, adults, and other council services.

Further regulatory requirements include, but are not limited to, Caldicott principles, the Transparency Code of Practice and the Section 46 Code of Practice under the Freedom of Information Act

Accreditation

Accreditation is the formal recognition that an organisation is competent to perform specific processes, activities, or tasks (which are detailed in a scope of accreditation) in a reliable, credible and accurate manner. These accreditations provide assurance to citizens and partners that we have appropriate measures in place to secure information.

We are committed to maintaining the following relevant accreditations, to ensure we meet minimum standards imposed by legislation and regulation:

- Public Services Network (PSN)
- Data Security & Protection (DSP) Toolkit (previously the Information Governance (IG) Toolkit)
- Cyber Essentials Plus
- Archives Service Accreditation

Information Assets

An information asset is a body of information that is valuable to our business regardless of the format e.g. paper, electronic, or microfilm. It will often be a collection of business information, for example information held in the social care system and any supporting files and documents would collectively be an information asset.

Managing information assets involves understanding what information is held, what is added and removed, how information is moved, and who has access and why. It is important that our information assets are properly managed so we can understand and address risks to the information and data, and ensure that information is only used within the law for the public good.

We will:

- ensure that information asset ownership and responsibilities are clear
- maintain a register of our information assets and owners
- rationalise our information assets and ensure their potential is maximized
- implement data quality standards
- continue to work towards a comprehensive overview of core business data, using tools such as the information asset register, register of processing activity (ROPA) and information flow mapping.

Lifecycle Management

The management of information in systems throughout its whole life; creation, storage, use and retention/disposal.

Many council staff spend a high proportion of their time creating, gathering or managing information. We can maximise the return on this investment in information by using it to inform the commissioning and delivery of services to Gloucestershire citizens.

We need to move away from a reliance on paper towards creating, storing and accessing all records in digital form in appropriate databases, shared drives etc, helping us to become a paperlite organisation. All new projects, processes and service reviews should store all key information electronically, where feasible.

We will:

Support Digital, Worksmarter and agile working

- Maximise the use of existing technology to help users manage and use information more effectively
- Implement data quality standards
- Take account of improved customer outcomes when designing and/or commissioning new information systems
- Improve the management of our information on corporate servers

Manage people's expectations about the use of their information

- Embed privacy by design
- Understand and document the reasons for processing personal data
- Ensure that data subjects are aware of the collection and use of their personal data

Ensure the provision of suitable storage solutions

- Develop and apply information lifecycle principles to our document and records stores
- Provide a records centre for the secure management of physical records
- Work to reduce the amount of information being stored
- Work towards a change of culture where key information is held for corporate benefit rather than in personal stores

Improve retention and disposal practices

- Improve retention functionality of our IT systems
- Maintain a records retention schedule
- Ensure secure confidential waste facilities are in place

Continue to identify and preserve key records

- Implement GCC's digital continuity policy to ensure continued and trusted access to information for current and future staff and customers
- Develop tools for the digital preservation of records
- Manage records of the council's major activities and decisions permanently in Gloucestershire Archives

Maximise the value of data and information

- Implement data quality standards
- Develop and implement a data analytics platform
- Make better use of data and collaborate to improve our strategic and operational insights

Transparency

There are increasing demands for transparency of public sector information. Each year we see a significant growth in the number and/or complexity of requests for information under Data Protection, Freedom of Information and Environmental Information legislation.

We will:

- provide dedicated resources to manage requests for information
- regularly review practices to ensure we are best placed to deal with the ongoing increase in volume and complexity of requests
- keep up to date with ICO guidance and decisions, and case law
- develop and upskill an internal network of key staff
- promote the public's rights of access to information on our website
- analyse requests to identify additional information that can be proactively published;
- publish responses to requests in a disclosure log
- publish information in accordance with the mandatory requirements of the Local Government Transparency Code
- look to open up our data to encourage those with digital skills to develop solutions for the public
- continue our programme of proactively publishing information and datasets to support requirements of openness, transparency and accountability
- ensure FOI responses provide access to information in a re-usable format.

Safe & Secure

The significance of information and related technologies is increasing in most aspects of business and public life, with the associated information security and cyber threats also increasing.

We therefore have a greater need to mitigate information risk and protect our information and related ICT assets from ever changing threats.

Security is an essential part of managing information. It is important that we embed an excellent user experience alongside sufficient security measures. We are developing our understanding of information risk management to encourage proportionate security measures that reflect a balance of the risks and the benefits. We are developing an holistic approach to protecting information through a combination of technical and non-technical security measures.

We will ensure appropriate organisational measures are in place, including:

- building security
- pre-employment checks that meet the Government standards
- secure transfer methods for physical records
- a cyber risk register
- a framework of policies, guidance and self-help tools
- a framework of council-wide business continuity measures
- contracts with our processors that are GDPR compliant.

We will maintain and develop appropriate technical measures, including:

- system security standards for new systems
- network protection, including firewalls, antivirus software and penetration testing
- data classification standards and tools
- secure channels for interacting with customers (e.g. Egress encrypted email)
- monitoring of information security controls used by our data processors
- understanding of security weaknesses and incidents, implementing improvements as required.

Information & Data Sharing

We work with a multitude of partners and suppliers and need to consider how information flows between us, ensuring any sharing is legal and compliant. To support this we need to embed information & data sharing agreements council-wide and ensure guidance and tools to facilitate partnership working are in place.

We will:

- commit to and support the Gloucestershire Information Sharing Partnership Agreement (GISPA) through membership of the Gloucestershire Information Governance Group
- promote use of the approved specific information sharing agreement template
- provide guidance to project managers, commissioners and contract managers to aid partnership working, implement privacy by design, reduce associated risks and ensure the whole information lifecycle is taken into account
- develop tools to enable an improved understanding of council information and sensitivities before it is shared, e.g. information flow maps
- provide a secure means to store, organise, share and access information (including, but not limited to, secure email)
- consider information implications and, where appropriate, undertake privacy impact assessments at the outset of commissioning services, major change projects or new contracts
- develop appropriate information governance, procedures and guidance before new technological solutions are implemented where feasible.

Information & Data Management and Analytics

We will take the approach that data will be moved from each system to a business analytics platform for transformation and reporting and analytics. This will be managed and maintained by the corporate Data & Analysis Team in a hub and spoke model working with analysts in the wider organisation to a common set of standards.

We will:

- provide a centralised data management service
- make reporting models made available to analysts
- ensure analysts have the data and tools they need to enable them to create and publish dynamic visualisations and dashboards
- make outputs available to other stakeholders such as team managers, heads of service, directors, members, partners and the wider public to access information on council performance, as appropriate; and
- ensure data management is governed tightly through principles of access permissions, working within the confines of the DPA and GDPR, and any other data and information security standards.

Training & Awareness

Education is key to bringing staff on the journey. Users are our last line of defence in securing the important information and data that we hold; all staff therefore need to be upskilled in managing information and data.

We will:

- ensure there are suitably qualified staff in place to advise the council
- develop appropriate analytical skills and capabilities within our analyst teams
- ensure our information asset owners understand their responsibilities
- deploy regular communications to our staff
- learn from security incidents, apply and share that learning
- upskill our staff in information and data management.

We will achieve this through:

- appropriate training for our information specialists
- annual e-learning for all staff
- use of MyCompliance tool to disseminate policies and key messages
- specialist training for key groups such as information asset owners, data analysts or those dealing with personal and sensitive information on a regular basis
- system specific training, e.g. SAP, ERIC, Liquidlogic, Capita One, Microsoft Power BI
- role based training, where appropriate.

Measuring Success

In order to know if the strategy is successful, it is important to have in place some performance measures, these include:

- Retaining PSN accreditation
- Retaining Cyber Essentials Plus
- Attain DSP Toolkit compliance (N3)
- Fines received
- Number of Information Asset Owners Trained
- Number of staff undertaken baseline cyber and information governance training
- Contact with the information security incident process
- Percentage of incidents rated moderate or above
- Number of incidents escalated to ICO
- Register of privacy impact assessments in place
- Number of privacy impact assessments completed
- Information asset register and register of processing activity developed
- Number of retention schedule reviews completed
- Number of information & data sharing protocols in place
- Number of contracts with GDPR compliant clauses
- Percentage of formal requests (FOI, EIR, SAR) responded within legal timescales
- Percentage of responses to formal requests resulting in a review
- Number of files held in the Records Centre

Roles and Responsibilities

Director: Strategy & Challenge (Senior Information Risk Owner (SIRO) and Chief Information Officer (CIO) – accountable for the effectiveness of the council's arrangements for managing and protecting information; ensuring that the council has adopted and implemented appropriate information management and security strategy, policies, assurance arrangements; and that the council has an adequately resourced and effective information management and security service. Responsible for information risk on behalf of the Chief Executive and Corporate Management Team.

Head of ICT – accountable for the effectiveness of the council's technical security arrangements and protecting information; ensuring that the council has adopted and implemented appropriate technical security policies and assurance arrangements; and that the council has an adequately resourced and effective technical security support service in place.

Head of Information Management Service & Data Protection Officer – undertakes statutory duties as set out in data protection legislation. Having due regard to the risk associated with processing operations, and taking into account the nature, scope, context and purposes of processing, the DPO monitors and audits compliance with GDPR and other data protection laws, data protection policies; ensures effective awareness-raising and training is developed and delivered; ensures that the council has an adequately resourced and effective GDPR support service in place; and act as a contact point for the ICO and data subject.

Strategic Intelligence Manager – responsible for the management and oversight of the business analytics platform, in collaboration with ICT; developing the analytical capabilities within the corporate Data & Analysis Team and the wider community of analysts throughout the council; developing a network of data champions and data quality stewards within areas of the business to promote robustness of data recorded within council systems; working with wider stakeholder groups to scope, develop and embed interactive data visualisations and analytics within service areas.

Performance & Improvement Manager – responsible for monitoring performance across council services; flagging concerns of poor data quality and recording practice alongside operational performance concerns; reporting to directors and heads of service as well as the Strategic Intelligence Manager and other interested stakeholders.

Caldicott Guardians – responsible for ensuring that the council satisfies the highest practical standards for handling person identifiable information in their area, supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information.

Information Board – responsible for developing and overseeing the council's approach to information strategy and governance, policy and standards.

Audit and Governance Committee – monitors the adequacy and effectiveness of arrangements in place for information management and security.

Information Asset Owners – responsible for undertaking information risk assessments; implementing appropriate controls and data quality measures; accountable for the systems they commission; recognising actual or potential security incidents; ensuring that policies and procedures are implemented and followed by users; and maintaining evidence of compliance.

Information Management Service – responsible for developing and maintaining a framework of GCC-wide policies, procedures and guidance to help colleagues manage the council's information assets effectively and securely; establishing and supporting data protection breach procedures; providing relevant training; maintaining corporate evidence of compliance; overseeing data security and protection toolkit submission; providing specialist advice and support.

ICT – responsible for providing technical security advice and support; developing relevant policies, procedures and guidelines; implementing and administering appropriate technical security controls; maintaining accreditation with PSN and Cyber Essentials Plus; and maintaining evidence of data protection compliance.

Gloucestershire Archives - responsible for gathering, keeping and sharing corporate and community archive collections relating to Gloucestershire and South Gloucestershire. As part of this role Gloucestershire Archives takes a leadership role in the long term preservation of digital information.

Data & Analysis Team – managing the analytics platform and embedding a uniform culture of analytics across the organisation, including data management standards within the platform and analysis standards within the data visualisaiton environment. Liaison with data champions and data stewards to ensure accurate, robust data are recorded within operational systems and available for reliable reporting.

Directors/Heads of Service/Service Managers – responsible for understanding and addressing information and data risks within their area; ensuring that appropriate arrangements are in place to manage information risk within their area, and within contracts and partnership arrangements; providing assurance on the security and use of those assets; and ensuring services have IAOs in place. Commissioning/Delivery Directors are responsible for assigning ownership of information assets to Information Asset Owners.

Staff – all staff are responsible for: managing and protecting the council's information assets that they handle; self development; engaging with training and applying learning; following policies and procedures; and recognising and reporting breaches of data protection.

Members – responsible for managing and protecting the council's information assets that they handle; and challenging council practices with regard to information and data management.

Service providers, contractors, partners and suppliers – responsible for complying with council policies, standards, contracts and partnership agreements. We expect the same standards as for our own staff.

Costs, increasing financial constraints, resources, time

In view of the large agenda and finite resources, it is necessary to prioritise areas of development activity in accordance with the associated risks. Priority areas for development each year are identified in the ICT, Information Management Service, Gloucestershire Archives and Planning, Performance & Change annual work plans and the annual Strategy & Challenge business plan.

Monitoring and Review

Ownership of this strategy rests with Information Board members who are responsible for agreeing, monitoring, promoting and reviewing its implementation.

Due to the pace of change, the strategy will be reviewed every other year, with the 1st review being due in April 2021.

An action plan will be developed to support this strategy, the key elements of which will be incorporated into the annual work plans for ICT and Information Management Service. Progress will be monitored quarterly. Monitoring will also include reports to Audit and Governance Committee, review of strategic risk registers, internal audits, external audits or peer reviews, where appropriate.

Further Information and Related Documents

Information management and security policies: https://www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-policies/information-management-and-security-policies/

Guidance for staff: https://staffnet.gloucestershire.gov.uk/internal-services/information-management-service/
(please note this link will not work for members of the public)

Digital Strategy: https://www.gloucestershire.gov.uk/media/1519646/2018-2023-digital-strategy.pdf

Gloucestershire Archives: https://www.gloucestershire.gov.uk/archives

Review

The next major review of the overall information strategy is due in November 2022.

Document Control

Author:	Jenny Grodzicka, Head of Information Management Service (DPO)
Owner:	Jane Burns, Chief Information Officer/Senior Information Risk Owner
Approval Body	Information Board
Date Approved	
Document Number:	V2-1

Version History

Version	Version date	Summary of Changes
0-1	2003, Jun	Information management strategy – primarily covering freedom of information, data protection and records management
1-0	2007, Sep	Information management strategy – substantial re-write setting out vision for next 5 years. Approved by Directors' Board, 5 Sep 2007
2-0a-b	2013, Sep	Draft information strategy v 2.0a and b for consultation
2-0	2014, Jul	Major revision setting out vision for next 5 years
3-0	2019, March	Information & Data Management strategy – substantial re-write, combining Information & Data Strategies, setting out vision for next 5 years. Approved at Information Board, 26 March 2019