Information Management Policy and Strategy

Document Owner: Executive Director of Corporate Services

Prepared by: Data Protection Officer

Version: 1.0 **Date: October 2021**

Contents **Page**

Version Number	Version Date	Version Description (Draft or Final)	Amended Section(s)	Name of Editor
1.0	Oct 21	Final		Nick Humphreys

1.0 Introduction

1.1 Information is critical to every part of the Council's operations.

1.2 Managing and using information correctly, protecting it appropriately and making it available to both stakeholders and the public enables the Council to fulfil its legal objectives, deliver improved services and reassures the public.

2.0 The Need for Information Management

2.1 Data and Information is everywhere and having the information at the right time is essential for the Council to operate efficiently, effectively and within legal parameters. The Council is a custodian of a wide range of data and the Council's role in service delivery and working in partnership has implications for how we manage information.

2.2 All of us, at all levels need to have the responsibility and accountability for the maintenance and use of all our information through its lifecycle – from creation to disposal of information and from paper to digital format.

2.3 Public sector organisations have more demands on them than ever before to be open and transparent.

2.4 The Council also has a legal duty to provide information requested by the public. If its information systems are in order, it will save staff time, enabling them to get on with their day-to-day work.

3.0 Vision and purpose

3.1 For information management to be successful, the culture of the organisation needs to place information management at the centre of its management arrangements.

3.2 Everyone has responsibility and accountability for the proper maintenance, security and use of information.

3.3 With updated and improved ICT platforms (SAP, Liquid Logic and Office 365) we must maximise the opportunities and benefits they offer. To do this, we need to manage our information effectively, re-use it where we can, share it appropriately and ensure that it is adequately protected.

3.4 This document covers all areas of the Council and all information, documents and data that we create, collect and hold in paper and electronic format. It covers all documents accessed by the public, staff, elected members and partners.

4.0 Key Principles

4.1 This strategy aims to ensure that information is managed in accordance with the following principles:

Information Management - Key Principles
Information is used legally. We will comply with relevant legislation around information, primarily the Data Protection Act 2018 and Freedom of Information Act 2000.
We are **open and transparent** about our use of information, informing customers what information we hold, and providing access to it, where allowed through legal channels.
Information is fit for purpose. Information is processed for a specified purpose and will be of sufficient quality and integrity to fulfil that purpose,
Information is used to its full potential. Within relevant legal frameworks information will be used to improve efficiency, reduce costs and improve the customer experience, while also supporting integration and redesign of services.
We will hold **no more data than is necessary** to fulfil a specified purpose. Where possible within legal frameworks, we will aim to ensure **information is created once** and accessed from a single point to provide a 'single record' and efficient use of the resource.
We will ensure data is **accurate, consistent and up to date** to support evidence-based decision making, service delivery and business intelligence.
We will **not hold data any longer than is necessary.** Where retention is necessary, we will digitise records moving away from the retention of paper and exploiting the greater security and accessibility offered by electronic storage.
We will ensure information is **secure** and **always protected** both at rest and in transit, from theft, loss, unauthorised access, abuse, and misuse.
All Council staff will be **accountable** and **responsible** for information management. We will provide staff with **guidance** and **training** on the requirements of Information Management.
We will **actively manage** information. Each Information Asset will have a designated **Information Asset Owner** (**IAO**) for each set of records/information, who understands the risks to that information and ensures staff manage the information in accordance with the level of risk.
We will be able to **demonstrate** our accountability through the maintenance of appropriate records and documentation. We will maintain **Records of Processing Activity (RoPA), Retention Schedules** and **Information Asset Registers (IAR)** providing details of the information the organisation creates, how it is used, and where it can be found.

4.2 Adherence to these principles will provide the following benefits:

Information Management Benefits
• Easier, more efficient, and accurate retrieval of information saving staff time
• Enhanced decision-making based on richer, higher quality and more relevant information, supporting the delivery of more efficient, cost effective services
• Better and more cost-effective use of storage spaces, as robust implementation of retention and destruction schedules enables records to be archived or destroyed as soon as they become inactive
• Working more efficiently, making better use of information assets; re-using information already created to support decision and policy making, service planning and integration
• Working more collaboratively, making better use of skills and knowledge
• Knowing what information can be shared, and with whom
• Knowing what information needs to be protected and what can be made available to partners and the public
• Provides assurance that risks are fully considered and managed, and that we are complying with legal and regulatory requirements
• Enables us to provide a more effective service to the public with greater transparency around the information we hold, enabling the public to participate in decision making
• Enhances our reputation with the public, and enables us to meet expectations of how we will manage their information

5.0 Defining Information Management and the Information Lifecycle

Information management is essentially the collection, storage, curation, dissemination, archiving and destruction of any source of information. Information can be defined as data in a context that allows for decision making.

Information goes through a set of defined stages in its lifecycle:

5.1 Creation or receipt

- Does the information need to be created in the first place?
- Has the same information already been created in another team or service or directorate? If so, can it be legally re-used for a new purpose?
- How long should the information be kept and why?
- Is the information digitised? If not, can it be digitised, and how?
- How should the information be classified and stored?

5.2 Use and maintenance

- What procedures are in place for the efficient storage and retrieval of the information?
- What are arrangements for maintenance, updating and amendment?
- How can the information be shared and tracked?
- Is the information personal or confidential? If so, where can it be stored securely?
- What backup and Business Continuity Recovery arrangements are in place?
- When is the information due for disposal or archive?

5.3 Disposal or archive

- Does the information need to be disposed of securely?
- Should the information be archived? If so, where, and how can it be stored?
- Will the information be usable/compatible in the future?

Information management seeks to ensure that all information is managed consistently and appropriately at every stage of its lifecycle, ensuring that confidentiality, integrity, and availability are maintained.

6.0 Roles and Responsibilities

All records that are created by staff of Sunderland City Council are Council records and as such are the property of the organisation, not the individual member of staff.

The Senior Information Risk Owner (SIRO), Caldicott Guardian and the Strategic Information Governance Group (SIGG) maintain oversight of council information management and risk. The Strategic Information Governance Group, chaired by the SIRO, is accountable for overseeing the implementation of this strategy. Executive Directors and Information Asset Owners are responsible for dissemination and implementation of arrangements within their service areas to meet these requirements.

Information Asset Owner responsibilities are held at Assistant Director Level.

Information Asset Administrators report to each Information Asset Owner.

6.1 Chief Officer Group (COG)

The role of COG members is to demonstrate leadership in the implementation of excellent Information Management arrangements in their area of control– ensuring this strategy is adhered to, reviewed and updated annually and satisfying themselves that service areas are appropriately resourced to ensure compliance is maintained and good practice observed.

6.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is an Executive Director who will take overall ownership of the Organisation's Information Management Policy, act as champion for information risk at COG and provide written advice to the Chief Executive on internal controls with regard to information risk.

The SIRO will assist the organisation to consider the information risks associated with its business goals and how those risks may be managed. The SIRO chairs the Strategic Information Governance Group (SIGG) and advises COG on the effectiveness of information risk management across the Council. The SIRO is responsible for ensuring that organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist.

The Executive Director of Corporate Services fulfils the role of SIRO for the Council.

6.3 Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patients (as service-users) information and enabling appropriate information sharing. The Guardian plays a key role in ensuring that the Council and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information. Their remit covers all health and social care records for children and adults.

The Caldicott Guardian makes sure that where confidential personal information is shared, for example with local NHS or other care partners, this is done properly, legally, and ethically in line with the following principles.

The Executive Director of Neighbourhoods fulfils the Caldicott Guardian role.

6.4 Data Protection Officer and the Data Protection Office

The Data Protection Office is responsible for:

- Advising Information Asset Owners on their Data Protection responsibilities.
- Reviewing and making recommendations for compliance with the Data Protection Act 2018, related legislation, and policies.
- Advising and raising awareness among staff on Data Protection obligations including responding to requests to exercise data subjects' rights, Privacy notices and Privacy by Design.
- Providing expert opinion to the business on the evaluation of risk and mitigation identified in Data Protection Impact Assessments (DPIAs).

- Monitoring compliance with Data Protection requirements.
- Providing advice, best practice guidance and training to staff on Data Protection and associated Information Management, and Access to Information.
- Coordinating activity to publicise and promote Data Protection and associated information governance principles, themes and issues across the Council.
- Supporting the Council in reusing and sharing information, in accordance with the Data Protection principles.
- Monitoring performance against Data Protection standards, identifying areas where improvements can be made.

Providing the Council's point of contact with the Information Commissioner's Office for:

- Consultation on high-risk proposals following a DPIA
- Maintaining arrangements for notification of personal data breaches

The Council has designated a Data Protection Officer to carry out the duties specified in the data protection legislation. The Data Protection Officer will report annually to the Audit and Governance Committee, and to each meeting of the Strategic Information Governance Group on compliance with Data Protection requirements.

6.5 Business Support

The Business Support function manages information inputs and retrievals from the archiving service contracted by the Council. The team also coordinates responses to Subject Access Requests and Freedom of Information (FOI) requests, Environmental Information Requests (EIRs) and provides the statutory Land Charges service.

6.6 Audit and Governance Committee

The Audit and Governance Committee receives the Annual Data Protection Officer report, and considers reports on Information Risk and Assurance, based on assurances from the Assistant Directors.

6.7 ICT and ICT security

The Chief Information Officer (CIO), in conjunction with the Assistant Director of Smart Cities has responsibility for assuring the integrity of the Council's Technology Architecture Strategy from a business assurance perspective. ICT provide advice and guidance to customers relating to Information Security and work with the Data Protection Office on the implications of technology or process change on Information Governance standards.

6.8 Assistant Directors - Managerial Accountability and Responsibility

Assistant Directors are responsible as **Information Asset Owners** for ensuring that the day-to-day management of information assets and staff meets statutory, regulatory, and Council requirements in support of this Strategy.

It is the responsibility of all Assistant Directors to:

- Support the Council's compliance with the requirements of relevant legislation including the Data Protection Act 2018 and UK GDPR, the Freedom of Information Act 2000.
- Support compliance with information management guidance, protocols and procedures, including ICT and Information Security requirements, through adequate resource allocation and training.
- Ensure that all information management advice, guidance, protocols and procedures are disseminated, implemented and followed within their service areas.

Under the Assistant Directors they must ensure that there is the responsibility of all senior managers to:

- Ensure staff receive appropriate training to meet their information management responsibilities.
- Ensure staff roles and responsibilities for information management are clearly explained and understood.
- Ensure the requirements of information management are clearly defined and scoped into future business plans.
- Ensure an information audit has been carried out within their area of work and that this is updated annually.

6.9 Employee Accountability and Responsibility

It is the responsibility of all employees to:

- Support the Council's compliance with the requirements of relevant legislation including the Data Protection Act 2018 and UK GDPR, the Freedom of Information Act 2000.
- Adhere to the Council's with information management guidance, protocols and procedures, including the Use of ICT Facilities Policy and Information Security requirements, and the Data Protection Protocols.

6.10 Wholly Owned Companies - Accountability and Responsibility

The Council's wholly owned Companies, their officers and staff are required to maintain compliance with the requirements of this strategy, and comply with statutory, regulatory and Council requirements and standards for the management of the information assets they process.

Contractual arrangements between the Council and its Companies set out that the Companies must provide information, access and assistance as necessary to enable the Council to meet its statutory obligations under the Freedom of Information 2000 and Data Protection Act 2018.

In particular, while the arrangements provide for the Companies to be either data controllers or data processors depending on the circumstances of the processing being carried out, they reiterate that the Council cannot divest itself of its data controller status, and associated liabilities, where that status is imposed on it by law for the delivery of the statutory functions of a Local Authority.

6.11 Elected Members – Accountability and Responsibility

Elected Members' Responsibilities fall within the following three areas of Councillor activity:

- Elected Members in their Council role
    - Members are required to observe the Council's requirements in their management and use of information, maintain compliance with the requirements of this strategy, and comply with statutory, regulatory, and Council requirements and standards for the management of the information assets they process.
- Elected Members in their Ward Councillor role
    - Members are the data controller in relation to personal information they obtain in the course of their Ward work and are responsible for determining the arrangements they consider appropriate in order to maintain compliance with statutory, and regulatory requirements and standards for the management of the information assets they process. Members are strongly recommended to adopt the Council's standards for management and use of this information and make use of the secure facilities provided to them, including use of encrypted devices.
- Elected Members in their political role
    - The Council has no role in determining or recommending how Members process information for political purposes. Members of political groups are regulated in this regard by the rules adopted by that group.

7.0 Strategic Information Governance Group

The Council maintains a Strategic Information Governance Group with the remit to maintain strategic overview of the Council's information governance arrangements, to facilitate information management liaison and consultation, across the Council and its connected companies.

The group has adopted terms of reference which are reviewed and updated annually to take in developments across the Information Governance arena. Within their terms of reference, the group maintains an overview of arrangements and compliance issues in relation to Data Protection, Freedom of Information, Records Management, Caldicott, Information Security and Regulation of Investigatory Powers.

Key Table of Advice

DPO	Business Support	Information Security	ICT Helpdesk
Data protection advice, including on: • Data Protection by Design and by Default, including Data Protection Impact Assessments • Advice on procurement of new systems • Data Sharing/Processor Agreements • Training content • Drafting policy/procedure/guidance for business approval FOI advice, including on: • Exemptions • Fee limits • Technical queries Primary point of contact with the ICO info.alert@sunderland.gov.uk for reports of known or suspected breaches and data incidents data.protection@sunderland.gov.uk for general DP queries and requests for advice	FOI coordination, logging and monitoring Subject Access Request coordination, and issuing responses Archiving and retrieval (via external provider)	IT security breaches Advice on technical security Advice on procurement of new technology ISO 270001 accreditation Cyber Security	Requests for service – business as usual

8.0 Training and Awareness

The relevance of information management to staff roles at all levels is a key message to be communicated across the Council. Information Asset Owners are required to regularly, and not less than annually, review the training needs of teams and individual staff and provide them with access to training to meet the identified needs.

The Data Protection Office will provide general training and awareness materials to officers across the Council. Training will cover Data Protection, Freedom of Information, Information Management and Information Security issues and will be delivered:

- To all new staff as part of their on-line induction process.
- Online, via the Learning Hub and Information Governance Service Hub on the Intranet.
- On request, where a service area identifies a requirement for specialist training.

9.0 Relationship with Existing Policies

This policy has been formulated within the context of the following Council policies:

Information Security Policy Framework

Sunderland City Council holds and processes information that is sensitive and confidential. Such information must be held securely and safeguarded from alteration, misinterpretation, loss, or theft.

ICT lead on the implementation of the ISO 27001 IT security standard. This standard provides guidance on the implementation of security measures within organisations, for the handling of its information, including the following:

- Information Labelling and Handling.
- Information Classification.
- Version Control and Tracking.
- Document Layout Standards.

Information Security Standards help identify, manage and minimise the range of threats to which information is regularly subjected.

Data Protection Protocols

These protocols set out the Council's measures for complying with the Data Protection principles set out in the Act, and for managing the information it holds fairly and lawfully, seeking to strike an appropriate balance between the Council's need to make use of information to manage its services efficiently and effectively, and respect the privacy of individuals.

- Partnership Working Protocol
- Privacy by Design Protocol
- Information Incident Protocol
- Data Transfer Assurance Protocol

10.0 Performance Measurements

There are a number of ways in which the Council can measure the effectiveness of its information management measures, by compliance to both statutory and non-statutory requirements and standards.

10.1 Statutory Indicators

Data breaches

- Known or suspected instances of a 'Personal Data Breach', as defined by Article 4 (12) of the GDPR to be reported to the Data Protection Team within 72 hours of coming to the attention of any Member or employee.

Information Requests

- All Subject Access Requests (SARs) to be completed within one calendar month
- All Data Subject rights requests to be completed within one calendar month
- All Freedom of Information requests to be completed within 20 (working) days
- All Environmental Information requests to be completed within 20 (working) days

10.2 Non-Statutory Indicators

Accreditation under ISO27001: This standard provides guidance on information security measures. The Council has achieved accreditation within the ICT unit.

The NHS Data Security and Protection (DSP) Toolkit: These standards support information governance practice in the management of health and social care records.

11.0 Supporting Materials

Below is supplied a list of the principal pieces of legislation, codes of practice and standards that guide the council's approach to implementation and adoption of records and information management practices.

11.1 Legislation

- Public Records Act 1958
- Local Government (Access to Information) Act 1995
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Re-Use of Public Sector Information Regulations 2005
- General Data Protection Regulation, implemented into UK law by the:
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

11.2 Codes of Practice

- Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000
- Local Government Data Handling Guidelines
- Regulation of Investigatory Powers Codes of Practice
- Covert surveillance and Property Interference
- Covert human intelligence sources

12.0 Resources

The following contain Information, Advice and Guidance on managing information:

- Information Governance Service Hub
- ICT Service Hub
- Learning Hub

13.0 Key Contacts

For further information, advice or guidance on any issues covered in this strategy please contact:

Data Protection Office

Nick Humphreys
Data Protection Officer
Email: nick.humphreys@sunderland.gov.uk
Tel: 07769 672633

Owen Thomas
Deputy DPO
Email: owen.thomas@sunderland.gov.uk
Tel: 07765 428155

Jackie Weeks
Deputy DPO
Email: jackie.weeks@sunderland.gov.uk
Tel: 07765 427631

Svetla Garchova
Information Governance Officer
Email: svetla.garchova@sunderland.gov.uk
Tel: 07765 428333

Team Email: data.protection@sunderland.gov.uk

Information Security - ICT

Richard Wright
Chief Information Officer
Email: Richard.wright@sunderland.gov.uk
Tel: 07766205544

Paul Thompson
Account Assurance Officer
Email: paul.thompson@sunderland.gov.uk
Tel: 0191 561 4870

Business Support

Wendy Anderson
Senior Business and Corporate Support Manager
Email: wendy.anderson@sunderland.gov.uk
Tel: 07435 662921

Paula Walker
Business Support Operational Manager
Email: paula.walker@sunderland.gov.uk
Tel: 07435 662937
Team email: access.files@sunderland.gov.uk

Martin Armstrong
Business Support Operational Manager
Email: martin.armstrong@sunderland.gov.uk
Tel: 07435 662927
Team email: recordsmanagementse@sunderland.gov.uk