Information Management Strategy 2017 - 2020

North Tyneside Council

1. Purpose of the Strategy

The purpose of the strategy is to set a direction for the effective governance, efficient management and use of information and data under the control of the Authority.

Information management deals with the creation, storage, access, protection and lifecycle of information and data. The introduction of the General Data Protection Regulation (GDPR) in May 2018 means that there is an increased need to focus on the overall value and accuracy of information, how it is used, stored and protected.

Information is central to the functioning of the Authority and its decision making processes, it therefore needs to be accurate and accessible to those who need it at the time and place that is required.

Under the GDPR the Authority will have a more stringent statutory duty to maintain records – in both paper and electronic formats – and to make its information available to the public as appropriate.

2. Strategy Development

North Tyneside Authority (NTC) first developed and published its Information Management strategy in 2013. Its purpose was to ensure that information was managed appropriately and successfully. This coincided with the introduction of the OpenText EDRM system. The first strategy led to some improvement in Information Management.

Increasing demands for the right to access information means the relationship between the public and the Authority is constantly evolving. This strategy has been developed in conjunction with key stakeholders including the Senior Information Risk Officer (SIRO), Caldicott Guardian, Information Security Group and Information Governance Team (IGT).

This revised Strategy sets out the Authority's approach to managing information to achieve the right balance between making information more accessible to staff to enable them to carry out their role effectively and more widely available to the public, whilst ensuring that adequate protection is in place.

The strategy aligns with the Authority's Creating a Brighter Future (CBF) programme which is a collection of key projects to deliver the policy priorities set out in the Our North Tyneside Plan. The CBF priority outcomes are:

- Ready for School
- Ready for Work and Life
- Cared for, Safeguarded and Healthy
- Great Place to Live, Work and Visit

The CBF programme will help to drive a major culture change and enable staff to work in a new way that will:

- Encourage our customers to be more independent
- Better manage demand for services so people access the right services at the right time
- Focus everything it does on delivering its priorities

3. Information Management Principles

Information is a valuable asset and contributes to the effective management of the Authority so that we can provide cost-effective targeted services that better meet the needs of our residents.

In order to protect the rights and interests of our residents when using their information the Authority has adopted seven Information Management Principles. This is required to enable compliance with the law, specifically the Data Protection Act and the General Data Protection Regulation (GDPR). These are:

1. Information is valuable and will be managed in a transparent and accountable way
2. Information will be collected once (where possible) in way that is relevant, accurate and consistent
3. Information will be organised to make it easy to retrieve and use
4. Information will be held securely and will be auditable
5. Information will be used to support Authority planning and decisions
6. Information will be shared where needed, in a manner that respects privacy
7. Information integrity, availability and reliability will be maintained until the information is no longer needed, at which point it will be destroyed

Each Principle is expanded below to explain why it is required, implications for the Authority, and possible exception or exceptional circumstances.

Principle	Implication	Exception
Information is valuable and will be managed Information is costly to collect. It will be treated as a valuable asset of strategic, operational and administrative value to NTC. We will do this in a manner that is transparent and accountable to the residents of NTC and the organisations we work with. And in order to maintain trust in our custodianship and use of that information we will comply with relevant legislation.	When we collect your information, we will need to maintain records of what was collected, under what permissions, and keep records of what that information is used for. We do this so that it is always accurate and up to date.	If information is 'open sourced' public information (i.e. it is publicly available from various sources), and can be re-obtained from source at low cost, NTC does not need to maintain it internally.
Information will be collected once, consistently and will be relevant Information is collected to document or facilitate the delivery of services in North Tyneside. We will collect information once (where possible), according to agreed standards that support relevance, accuracy and consistency so that it is fit for purpose, reliable and can be, where	Information should be gathered in a structured form. Where it is collected it should be relevant to the purpose – and collection of extraneous information should be challenged. Where possible, the information should be cross-checked with other information and verified in order to prevent proliferation of partial records (e.g. alternative name spellings,	Under the GDPR it is a requirement that all information must be relevant to the purpose, there will be no exceptions to this aspect. Some information may be 'narrative' for particular purposes (e.g. the child's story in Social Care) and/or personally sensitive.

appropriate, re-used by the Authority to improve service delivery or management reporting.	multiple addresses).	Sometimes this information may not be structured and does not always require validity checking.
Information will be organised to make it easy to retrieve and use We will organise information in a manner where it is described and linked to related information such that it is easy for NTC employees to search, retrieve and use.	Organisation of information requires it to be categorised, so that it can be associated with related information (e.g. 'legal cases' or 'information concerning Mrs Jones'), so that it can be identified and re-used. This should be through a standardised approach such as the Local Government Classification Scheme. Unstructured information can be searched, but relevancy and control become extremely difficult, and risks contravention of the GDPR.	Short term notes are often convenient for local explanations and/or exploration of ideas. This may not be highly organised. Where non-personal, this should be deleted after use in favour of structured records. Where it concerns an identifiable individual, records may need to be kept but this should be attached to a structured location for audit purposes.
Information will be held securely and will be auditable Our information will be stored in a secure manner to prevent unauthorised access, alteration, loss or deletion. Our information will be auditable so NTC can demonstrate to its residents, organisations we deal with, central government and the Information Commissioner that we protect sensitive	As a valuable asset not just to the Authority but to our residents and the organisations the information concerns, we are required by law to protect that information both for purposes of confidentiality and integrity. This means that control over access to information should be compliant with the GDPR and	Information may be non-personal and/or non-sensitive. Such information may not be relevant after its initial use (e.g. a monthly information report). There is no reason to retain or track the destruction of such information.

data and information.	Caldicott requirements, including its encryption and the management/audit of any changes, including deletion.	
Information will be used to support Authority planning and decisions We will use information effectively to support planning, decision making, resource allocation, reporting, communications and transactions. Information will be processed and analysed by NTC to develop evidence-based policy and deliver targeted services to our residents. Information will be re-used where appropriate, so NTC derive maximum benefit from it.	If information is unused, there is no value in holding it. If the Authority takes decisions on poor information, then we may be providing the wrong services, or worse, missing an intervention in a high risk situation. The Authority will ensure it uses all the tools it has available to make sure that residents are provided with the right services at the right time (consistent with privacy and consent) which means we should be exploiting the information we have collected.	At certain times strategic decisions may be made that take into account available information that may go beyond the evidence in order to achieve the desired outcome.
Information will be shared where needed, in a manner that respects privacy We will respect the rights and privacy of individuals and organisations when we share information. Where we have a Statutory duty to do so we will only share information where appropriate to reduce duplication of effort, streamline service delivery and provide a	We must have a rationale, compliant with individual's consent or with law, for each occasion on which we share information. This means that we should have a system of recording that consent and/or the rules by which we are publishing that information such that we can transparently demonstrate	The sharing of information is covered by data protection law, and the Authority must maintain compliance with law. The Authority can choose not to share information within itself or with other parties where it considers that the risks of doing so exceed the benefit derived; however, this should be minimised and

consolidated view of our residents' needs or public sector performance. Where appropriate, we will publish information for discovery so that we demonstrate transparency thus providing opportunities to communicate, consult and collaborate or to engage in value-added processing, analysis and development.	compliance and retain trust in our custodianship.	those exceptions should be clearly recorded.
Information will be maintained We will preserve the integrity of our information using cost-effective, risk-based measures that facilitate business continuity. We will ensure the availability and reliability of information for as long as it is needed to support service delivery and accountability. We will destroy information when its use and value has ceased to minimise the costs and risks to NTC and to respect the rights of our residents.	There are a number of implications of maintaining integrity, availability and reliability particularly around maintaining an auditable track of who has accessed that information; and controlling who has the right to access that information, and ensuring that the information remains available even after a major incident such as fire or flood. As the above processes are costly, it is reasonable to destroy the information no longer needed to minimise those costs, otherwise the Authority's costs will inexorably rise with no benefit to services. It is also required in law that we should not hold personal information longer than required.	If information can be regenerated from another (reliable) source relatively easily, there is no need to locally maintain multiple copies.

Principles previously set out in the 2013-2017 strategy have been updated to reflect the GDPR. This will ensure the Authority sustains a focus on the important elements of information management so that the public can maintain trust and confidence in the way the Authority operates and handles information.

As part of the significant improvement in information management arrangements within the Authority, a Senior Information Management Forum (SIMF) was created in 2014. Part of the role of this Group is to oversee and govern the delivery of the Information Management Strategy.

4. Moving forward

The Information Governance Team (IGT) has lead the work and provided the focus for the Authority's activity in this area. The IGT will lead in the creation of a new Information Governance work streams for 2017 - 2020, that will focus on strategic initiatives that can be delivered. This will include preparing the authority for the forthcoming General Data Protection Regulation which comes into force in May 2018 and leading on the Information Governance strand of the Office 365 project.

Information is used across all service areas in the Authority to achieve the objectives set out in the North Tyneside Plan. Information is held in the Authority in a variety of printed and electronic formats including policy documents, reports, minutes, statistics, operational data and personal data. The IGT will review this to ensure it meets with relevant legislation.

Alignment with the Creating a Brighter Future (CBF) and Our North Tyneside Plan

The CBF and Our North Tyneside plan define where we focus our energies and resources, how we will judge our performance and the Authority's contribution to the welfare of the economy and its residents. The planned actions in the Information Management Strategy 2017-20 have been aligned to these to achieve the vision in the plan.

The guiding principles are:

Our people will

- Be listened to, and involved by responsive, enabling services
- Be ready for school – giving our children and their families the best start in life
- Be ready for work and life – with the skills and abilities to achieve their full potential, economic independence and meet the needs of local businesses
- Be healthy and well – with the information, skills and opportunities to maintain and improve their health, wellbeing and independence
- Be cared for and safeguarded if they become vulnerable

Our places will

- Be great places to live, and attract others to visit or work here
- Offer a good choice of quality housing appropriate to need, including affordable homes
- Provide a clean, green, healthy, attractive and safe environment
- Have an effective transport and physical infrastructure - including our roads, cycleways, pavements, street lighting, drainage and public transport

Our economy will

- Grow by building on our strengths, including our existing companies, and small and growing businesses

- Have the right skills and conditions to support investment, and create and sustain new, good-quality jobs and apprenticeships for working-age people

To maximise the potential benefit of the information held, the Authority will manage it effectively, re-use it where it can, share it appropriately and ensure that the strategy aligns with the priority outcomes of the Authority Plan.

The Authority recognises that in order to achieve its priority outcomes in the Authority Plan, the information management objectives need to focus on the following:

- Protecting information – the Authority relies on information to be able to carry out its functions. The Authority processes service user and employee data and more and has a duty to put necessary measures in place to protect that information.

- Sharing information – the Authority has an obligation to share information under Freedom of Information legislation. It also has a duty to protect its confidentiality in certain situations however there will always be certain situations when the sharing of personal information is essential.

Information Management Objectives aligned with Strategic theme 1 (People)

Improving the way the Authority manages its information results in delivering a seamless user service. This will enable the Authority to deliver the tangible and visible benefits in an effective way to:

  - Raise public confidence in the way the Authority collects, manages and uses personal information
  - Know what information the Authority can share and how to share for legitimate purposes
  - Provide assurance that risks are reduced and that customer's information is safe with the Authority.

- Reducing levels of information-related risk and ensuring that information is protected and secure
- Ensuring that good information rights practice is embedded into the culture and day to day processes of the Authority and into emerging technologies and systems.

Information Management Principles aligned with Strategic theme 2 (places)

- Ensuring compliance with legislation.
- Improving data quality.
- Improving informed decision making and policy development.

Information Management Principles aligned with Strategic theme 3 (Economy)

- Ensure that we develop the Publication Scheme so it includes information which will provide the information individuals and businesses need to inform their decision making
- Continue to promote transparency by responding to 'requests for information' in a timely manner.
- The Authority will continue to deliver its statutory duties in relation to information management by:

    - Managing the Authority records with care under relevant legislation;
    - Considering the reuse of public sector data under the Re-use of Public sector Information Regulations 2005

The Approach

A range of development work will be undertaken to deliver effective information management practices throughout the Authority. This will ensure the Authority's information resources are protected from risks and threats. This includes:

- Training and awareness - staff are required to undertake mandatory IG training
- Information governance – controls are in place to ensure compliance with the DPA and forthcoming (General Data Protection regulation).
- Records and information management - effective processes are in place to manage the Authority's records and information.
- Data sharing – the sharing of personal data complies with the principles of the DPA (and forthcoming General Data Protection Regulation) and the Information Commissioner's Data Sharing Code of Practice.
- Information Security –information security processes are in alignment with ISO:27001 and the Authority's Security Policy Toolkit and security processes are clear and accessible.

- Monitoring and assurance – this will be carried out in accordance with the Authority's policies and guidelines to give assurances to Senior Management and Cabinet.

Reporting, monitoring and reviewing

The IGT own and are responsible for this strategy. Implementation rests with all staff. An annual action plan will be developed to deliver this strategy. This will be monitored on a regular basis by the Information and Records Manager, SIRO and Deputy SIRO. Monitoring will also include regular reports to the SLT and SIMF.

Information Management Framework and Assurance Policy

The Authority Framework and Assurance policy sets out the relevant roles, responsibilities, policies and procedures, along with best practice and standards for managing the Authority's information assets. It also describes the approach to assurance and risk management and to IT Security.

Key roles

Chief Executive

The Chief Executive has overall corporate responsibility for Information Management within the Authority.

Senior Information Risk Officer (SIRO) and the Deputy SIRO.

The SIRO responsibility has been assigned to the Authority's monitoring officer. The SIRO is also a member of the Strategic Leadership Team and leads on Information Risk management for the Authority. The Deputy SIRO, also the deputy Monitoring Officer, assists the SIRO in the decision making process.

Strategic Information Management Forum (SIMF)

The SIMF is chaired by the SIRO or the Deputy SIRO. The aim of the Group is to have a corporate oversight and responsibility for information issues. The group meets every quarter (or more) to oversee the Authority's information management function.

Information Asset Owners

The Information Assets owners (IAOs) have the responsibility for the information lifecycle in their department. This includes a comprehensive list of all information sharing, information risks and information management within their department. The Head of each department is the nominated Information Asset Owner. The assets owners are supported by Deputy Information Asset Owners (Deputy IAOs) or the

Senior Managers who will assist in delivering this function to the respective individual services.

Information Security Group

The key responsibility for the Information Security Group is to ensure that the Authority has suitable measures in place for secure and effective handling of vital and sensitive information including personal information.

Details of the key roles and others plus their responsibilities have been outlined in the Information Management Framework and in the Terms of Reference of the relevant working Groups.