Havant
BOROUGH COUNCIL

Information Governance Policy, Strategy and Framework

Author	Cheryl Lincoln
Effective Date	December 2019
Review Date	December 2020
Version	V2.0

Version Control

Version Number	Date	Author / Reviewer	Comments / Changes
V0.1	01/12/2017	Cheryl Lincoln	First Draft
V0.2	19/02/2018	Cheryl Lincoln	Updated following feedback from Information Governance Board
V1.0	19/02/2018	Cheryl Lincoln	Approved by Information Governance Board
V1.1	16/06/2019	Cheryl Lincoln	Review and Update following IG Internal Audit and IGSG feedback
V2.0	13/09/2019	Cheryl Lincoln	Approved by Information Governance Board with minor amendments.

Dissemination

Who?	Method	Date	Version
All Staff	Team Talk / Email to Team Managers		2.0

Publication of current version

Version	Location	Date
2.0	Website / Intranet	

Approval of current version

Author / Reviewer	Who / Board	Date	Version
Cheryl Lincoln	Corporate Governance Board	24/09/2019	2.0

Table of Contents

1. Management Summary

Heads of Service (Information Asset Owners) are *accountable* for their Service areas and Managers/Team Leaders (Information Asset Managers) are *responsible* for ***all*** that happens in their teams, in particular Managers/Teams Leaders are responsible for all information in their areas which includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction of Information or data.

The definition of information and what it covers is contained on page 7.

This Policy is in 3 parts: -

1. The Policy (from page 8)
   are the regulations we are bound by and principles/procedures that the organisation has agreed to
2. Framework (from page 13)
   the measures in place to manage information appropriately
3. Strategy (from page 20 and Appendix 4+5)
   a plan of action designed to achieve a long-term or overall aim.

This document will give you the details of why we must manage our information and how we must manage our information.

2. Introduction

Public authorities rely on the collection of an ever-increasing amount of information to inform their strategies and plans to provide community and regulatory services. This document sets out the framework within which the council will promote a culture of good practice around the processing of information and the use of information systems and details the agreed policy for achieving this.

Information is a valued corporate and public asset and a key resource required to deliver the Council's business objectives and to meet the expectations of our customers. Moreover, the Council needs to be open in the way it does its business; in how it delivers its services to its customers and in how it makes decisions.

As part of the 6 Councils Contract, Capita deliver a significant number of services on behalf of the Council. As the partnership with the other councils grows and develops there will be changes to the policies and governance documents, as a result this framework will be updated to reflect those changes to ensure local documents support 6 Councils harmonised policies.

3. Purpose

The purpose of an Information Governance Framework is to formally establish the organisational approach to Information Governance. It also sets out the principles for controlling the information lifecycle from creation to disposal and will enable the Council to better meet the needs of the public and be an open and accountable organisation. In effect, Information Governance refers to a policy and/or framework outlining acceptable behaviour for managing, organising and sharing information, data and files and incorporates roles, processes, and standards.

When we are talking about Information Governance we are also talking about Information Management. These words are often seen as interchangeable, although the governance element is more about ensuring compliance with rules and procedures, particularly if they are regulatory.

Effective information management results in the Council keeping information (both personal and non-personal) safe and protecting the interests of residents and service users. The purpose of this document is to provide a framework for managing the Councils information to enable the Council to:

- Deliver quality services by having timely access to meaningful and appropriate information
- Make informed decisions
- Be open and transparent
- Respond appropriately to information requests from the public
- Protect vital records
- Comply with relevant legislation
- Work with partners

Information management has become an increasing challenge for local authorities due to the continuing development of technological advances, legislative requirements, joint working/partnership arrangements and central government requirements. Information is also evolving from different mediums e.g. social media (Facebook, Twitter, WhatsApp). The Council needs to ensure that any information produced by its staff is created and managed in a secure, professional way. All information that is produced on behalf of the Council is a corporate resource and belongs to the Council. It forms part of the Council's Corporate Memory and must support the business needs of the Council.

4. Background

There are several major initiatives that the Government have instigated such as improving transparency and the greater use of partnerships to deliver services and solve problems. The government is demanding transparency from the public sector and to make more information proactively available. This greater demand for openness and transparency means that information must be easily accessible and able to be extracted. Information management and governance has important implications for the success or failure of each of these initiatives. According to the Society of Information Technology Managers, managing information is managing the lifeblood of the organisation. There has been a raft of new legislation in the last few years which has placed new obligations on Councils. There are regulations that require us to provide information within given time scales, to make information more accessible and to guard people's rights. In order to comply we must ensure we manage our information effectively, taking into account these new legal requirements. The list of legislation below affects some or all services and are drivers for Information Governance:

- Data Protection Act 2018
- General Data Protection Regulation
- Human Rights Act 1998
- Freedom of Information Act 2000
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2004
- Environmental Information Regulations 2004
- Local Government Transparency Code of Practice 2015
- Protection of Freedoms Act 2012
- Intellectual Property Act 2014
- Local Government Acts 1972 – 2003
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 + Investigatory Powers Act 2016
- Misuse of Computers Act 1990
- Consumer Protection Regulations 2000
- The Electronic Commerce (EC Directive) Regulations 2002
- Re-use of Public Sector Information Regulations 2015

5. Scope

In order to comply with legislation and to ensure the Council manages its valuable information assets effectively, the Information Governance framework covers: -

a) Systems: All Information systems within the organisation (both electronic and paper based) fall within the scope of this framework
b) Staff: All users of council information and/or systems including council employees and non-council employees who have been authorised to access and use such information and/or systems.
c) Information: All information and data collected or accessed in relation to any council activity whether by council employees or individuals and organisations under a contractual relationship with the council. All information stored on facilities owned or managed by the council or on behalf of the council.

Information, in all its forms, whether electronic, paper-based or in people's heads, is our second most important resource after our people. Information is a corporate resource, to be shared and used as effectively as possible, it is ***not*** owned by the individual who created it but by the authority, the authority is the Data Controller.

Failure to manage information properly within the organisation exposes the council to a significant financial, legal, public relations and potentially manpower-shortage risk. When reviewing or implementing technologies, Information Governance should be a consideration. To help develop this Strategy, the Council has accepted that there will be multiple DMS solutions, service led, which will be developed and implemented.

When talking about information, it covers all information in all formats i.e.

- On paper
- In corporate systems such as Integra and Geographical Information System (GIS)
- In departmental systems such as Acolaid, Lalpac, Iken and Mosaic
- In documents produced by desktop applications such as Microsoft Office (Outlook, Word, Excel etc.)
- On the council's intranet and public website
- CCTV footage
- Audio and Video Files

There is a great deal of confusion between Information Technology and Information Governance. This has led to relatively too much effort being spent on managing information technology, and relatively too little spent on managing information. Information Governance is concerned with the actual meaningful content that we own and how that content is prepared, and its quality ensured. Information Technology helps with the dissemination and spreading of that content, but the entire Information Technology infrastructure in the world is of no use if the core content is of poor quality.

To take an analogy from the publishing world, Information Governance is analogous with the writing and editing of a book, whereas Information Technology is analogous with the printing and distribution of the book. Both processes are important, but Information Technology must always support the Information Governance, not the other way around. Information Technology is not Information Governance.

The objectives of this framework are: -

A. To instil an understanding, of the importance and the potential of, effective information governance.
B. To help develop awareness, understanding. and to promote the application of good practice in handling information and the development of skills in this area.
C. To define what the council considers are the principles and practice of good information management and to reduce risk.
D. To support the council's ambition to improve processes, to improve customer services, to become more efficient and to reduce costs.
E. To ensure that the council takes advantage of technology advances appropriate to conducting the Information Governance processes within the council.
F. To ensure business continuity and protect vital records to ensure the continued functioning of the Council if any disasters affect the Council

6. Information Governance Policy

6.1. The council will comply with legislation and other mandatory standards

The council is committed to continuously improving the way it responds to requests for information under statutory access regimes, including the Freedom of Information Act 2000, the Data Protection Act 2018, the General Data Protection Regulation, and the Environmental Information Regulations 2004. Compliance, however, is reliant upon proper management of the council's information, which needs to be managed, secure and easily located. The council regards all identifiable personal information relating to residents/customers as confidential and all identifiable information relating to staff as confidential (except where national policy on accountability and openness requires otherwise). The council complies with: -

- **Data Protection Legislation** (GDPR and DPA2018) which relates to personal identifiable information. (See Data Protection Policy for more information)
- **Environmental Information Regulations 2004** which relates to requests about the environmental (air, soil, water, environment i.e. Planning etc.). (see Access to Information Policy for more information)
- **Freedom of Information Act 2000** relates to requests not covered by the above (see Access to Information Policy for more information)
- **Common law of confidentiality**. (See staff IG Handbook for more information)
- **Local Government (Records) Act 1962 / Local Government Act 1972 and Lord Chancellor's Code of Practice for Records Management** relates to the local authority having records management policy and procedures in place

6.2. The council will promote open information

The council will promote transparency and open information by: -

6.2.1. Access to Information Policy

The council will maintain an Access to Information Policy which will describe the arrangements and practices that are in place to ensure that the council can respond appropriately to information requests. The council will also ensure there is greater openness of decision-making; that the council builds the trust of the public; and provides clarity on the way duties will be met under access to information legislation, guidance and best practice.

6.2.2. Publication scheme

The Publication Scheme provides a list of documents routinely requested by the public. It is organised into 'classes' of information examples are

- 'Who we are and what we do' and will include: - Organisational information, locations and contacts, constitutional and legal governance.
- 'What we spend and how we spend it' and includes: - Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

6.2.3. Re-use of Public Sector Information

The Re-use of Public Sector Information Regulations (2015) do not provide access to the information itself, it focuses on the re-use rather than access. The Regulations require the council to ensure that a list of significant documents available for re-use is made available to the public, preferably electronically. Requests for access to information will be dealt with under the FOIA, DPA, GDPR, EIR and other information access provisions.

6.2.4. Individual's Rights Handling Procedure

Under Data Protection legislation the council will maintain a 'Guide to Subject Access Rights' that describes the arrangements and practices that are in place to ensure that the council can respond appropriately to any request made in relation to Individual's Rights. It will also provide clarity on the way in which the council will meet its duties under the Data Protection Act and the General Data Protection Regulation, guidance and best practice.

6.3. The council will commit to information security and confidentiality

6.3.1. Physical and electronic assets

The council is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the Council. Information and information security requirements will continue to be aligned with the council's goals. The framework of security policies is intended to be an enabling mechanism for information sharing, electronic operations, and reducing information-related risks to acceptable levels. In particular business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to the success of this policy.

The diffusion of technology into our daily working environment has meant that data security has become an Executive Board issue. There is more focus on the transparency of public data than ever before with the intention that publishing data will strengthen accountability to residents. At the same time, central government data losses and the continuing emphasis in the press around breaches of data security require the council to reinvigorate its response to data security.

6.3.2. Security Policy Framework

This policy should be read in conjunction with the ICT Security Policy which sets out the overarching approach to Information and Communication Technology (ICT) policies in the council and are listed in the Governance Framework section on page 14 below.

7. Measures in place for Information Assurance

7.1. Overview

Information assurance describes the measures that are in place to ensure that the council meets the requirements for good information governance, individual roles and responsibilities are detailed in section 12.5 below. This section, therefore, describes how the governance arrangements will operate to ensure that this is achieved.

7.2. Corporate Governance Board will receive reports on information governance

The Corporate Governance Board will receive quarterly reports from the Information Governance Steering Group that relate to information governance and data security as appropriate. These will be presented by the chair of the Information Governance Steering Group, who will also serve as the council’s Senior Information Risk Owner. The Corporate Governance Board provides assurance to the Executive Board.

7.3. The Information Governance team will raise risks as appropriate

The Information Governance Team will raise risks related to information governance and report these as appropriate:

a) The Information Governance Team will determine when risks ought to be escalated to the Information Governance Steering Group and will prepare reports for this board as necessary.

b) The Data Protection Officer will respond (reactively) to data security incidents as they arise and manage a process of improvement (proactively) through the 5 Councils Security Working Group. The Data Protection Officer will also provide assurance and highlight risks to the SIRO.

c) The Information Governance Manager has corporate responsibility for access to information requests and information complaints and will determine the processing of these in accordance with the council’s responsibilities for records management. The Information Governance Manager will provide assurance by chairing an Information Governance Champions meeting at least four times a year, where matters will be raised, and risks discussed. The Information Governance Manager will provide reports on the council’s compliance with access to information requests and these will be reported quarterly to the Information

Governance Steering Group and onward via the Quarterly Health check to Councillors.

d) The Information Governance Officer has day-to-day responsibility for access to information requests and to ensure that information requests are managed and processed according to the council's responsibilities for records management. The Information Governance Officer will facilitate quarterly Information Governance Champions meetings ensuring that matters can be raised, and risks discussed. The Information Governance Officer will also produce reports on the council's compliance with access to information requests and provide these to the Information Governance Manager.

7.4. Service Areas will be represented at Information Governance Champions meetings

Service areas will ensure that there is appropriate representation at the council's Information Governance Champions meetings.

7.5. All staff will be trained on data handling and good information governance

All staff will be trained on data handling, security and appropriate information governance. All training will be coordinated by the Data Protection Officer, who will ensure there is an auditable record of training completion.

7.6. There will be good awareness of information governance matters

The Information Governance Team will ensure that there is an ongoing mechanism for maintaining good awareness of information governance matters. This will comprise:

- Updated information on the council's intranet
- Promoting Data Protection and Cyber Security E-Learning
- Regular articles in Team Talk and/or Weekly Email
- Attending Team meetings
- Annual review from staff of the Information Governance Handbook
- Training specific groups of staff within specialist areas

7.7. A records management policy will be maintained[1]

The council will maintain a records management policy that sets out a corporate policy for the management of records within the council to ensure compliance with the Local Government Act 1972, Data Protection Act 2018, the General Data Protection Regulation and the Freedom of Information Act 2000. The policy defines roles and responsibilities and sets out the standards of corporate records management (retention schedule, classification scheme, DMS and records destruction). The Records Management Policy will be updated routinely by the Information Governance Team and approved by the Corporate Governance Board.

7.8. A Corporate Records Retention Schedule will be maintained

The retention schedule sets how long records need to be stored before we can or should destroy them. The council's retention schedule is built on the retention

[1] Under review

periods given in the Local Government Classification Scheme (LGCS). Changes to these retention periods, where required, will be approved between service areas and the Information Governance Team.

7.9. Information sharing protocols will be updated and in place

All local Information Sharing Agreements will be quality assured by the Information Governance Team who will decide whether or not the agreements require approval by the Information Governance Steering Group.

7.10. Reporting Incidents

All faults must be reported to the IT Helpdesk in line with the council's Security Incident Management Procedure. It is the duty of all council staff and all other users of council equipment to immediately report any actual or suspected breaches in information security.

8. Policy Compliance

All employees are expected to serve the council and implement its policies to the highest standards, as described in the Code of Conduct. If any user is found to have breached this policy, they may be subject to the council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, please seek advice from the Information Governance Team.

9. Governance, Approval and Review

This policy will be formally signed off by the Corporate Governance Board; who provide assurance to the Executive Board. It will be reviewed on an annual basis by the Information Governance Team and annual approval will be by the Information Governance Steering Group.

10. Aims of Information Governance

The successful implementation of the Strategy and Framework will assist the Council to:

- Fulfil its statutory obligations including those relating to the disclosure of information under Data Protection legislation, Freedom of Information Act and Environmental Information Regulations in the most cost-effective way.
- Have accurate and up to date information to support Council operations and decision making.
- Hold, process and manage information in a secure way.
- Empower employees to be well informed about good information management practice.
- Produce consistent, accurate, timely and comprehensive data by collecting information once and using it numerous times.
- Provide staff and councillors with access to the information they require to fulfil their duties in accordance with appropriate security and access policies.
- Improve information management within the Council.

- Provide value for money by using information effectively and avoiding duplication of time and resources.
- Only collect information when it is necessary.
- Be an organisation which works to a clearly defined and implemented Information Asset Register which is reviewed regularly.
- See information as a resource to the whole organisation and share as appropriate to increase consistency, avoid duplication and remove unnecessary storage.
- Increase effective partnership working by facilitating appropriate information sharing.
- Ensure information security of the appropriate technical systems is protected in accordance with legislation.

11. Information Management Principles

Information Governance is at the heart of the way in which we deliver services to the public and enables us to discharge our responsibilities for public accountability. If we do not have consistent and accurate information, we cannot work efficiently or measure the improvements; to achieve this, our information will be:

A. **Available** - Our information will be available to those who need it, when they need it and who have the permissions to view or use it. This will include dealing with requests for information.

B. **Accessible -** Our information will be clearly identified and easily found when it is needed, in a timely fashion, by anyone with authority who needs to access it.

C. **Electronic** - Our information and documents will be stored electronically. Over time, we will evolve such that we will endeavour to only keep paper records where there is a legal requirement to do so.

D. **Secure** - We will ensure that there are controls in place when we store and transfer information, so that the information itself is protected and any risks associated with inappropriate disclosure are reduced. We will record the confidentiality of information.

E. **Managed throughout its lifecycle -** It is essential that information is only kept for as long as necessary, whether it is through a legal requirement or a business need. Information when it is no longer required should be disposed of in a secure manner in line with our retention and disposal policy.

F. **Generate an information culture** – Information should be managed in a common structured system. This encourages collaborative working and reduces duplication of work.

G. **Information assets** - make full use of our information assets

H. **Training** - Implement a training programme to encourage staff to manage, share and work with information in a corporate way to ensure all the above.

12. The Governance Framework

12.1. Overview

The Information Governance framework describes the measures in place to manage information appropriately to support the council's ability to deliver efficient services. The framework comprises of four areas as follows: -

- Measures in place to ensure legal compliance
- Stated information governance policy measures in place
- Good information governance assurance mechanisms that are in place
- Duties and Responsibilities that are in place within the council

12.2. Measures in place to ensure legal compliance

The Framework sets out the council's policy towards information governance, including the council's information standards. There is a Data Protection Policy and Access to Information Policy in place to ensure the council meets its legal obligations in respect of the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the Re-use of Public Information Regulations 2015, Data Protection Act 2018, the General Data Protection Regulation and the statutory rules concerning access to information about council meetings and papers, including those of the Executive. This policy also sets out the governance framework, including setting out the key roles and responsibilities and the arrangements for training, monitoring and review in relation to each of these areas.

12.3. Stated information governance policy measures in place

The council will ensure that it has policy measures in place to enable good practice around the handling of information; promote a culture of awareness and improvement; and, complying with legislation and other mandatory standards. These are described in Section 6 above the 'Information Governance Policy'.

To support the council's commitment to good information governance, the council will also abide by the following other information policies and procedures and these will be updated regularly: -

ICT Security Policies: -

a) Information Security Statement
b) Password Policy
c) Acceptable use Policy
d) Email Policy
e) Removeable Media Policy
f) Risk Management Policy
g) IT User Policy

Information Governance Policies: -

a) Data Protection Policy
b) Access to Information Policy
c) Retention Schedule

To follow: -
Records Management Policy
Information Asset Owner Policy

12.4. Good information governance assurance mechanisms are in place

The council will ensure that it has measures in place for monitoring information governance and escalating issues and concerns as they arise. These are described in the Section 7 above ‘Measures in place for Information Assurance’.

12.5. Duties and Responsibilities are in place

The council will detail the roles and responsibilities that need to be in place to ensure adherence to good information governance arrangements and these are described in the following section: -

Key Roles and Responsibilities

- **The Information Governance Steering Group (IGSG)**

The IGSG is responsible for overseeing Information Governance, Security Policy Framework, information compliance and records management. The IGSG is chaired by the councils Senior Information Risk Owner (SIRO).

- **The Senior Information Risk Owner (SIRO)**

The SIRO is responsible for setting strategic direction in relation to information governance and security related matters. The SIRO understands the strategic business goals of the council and how business goals may be impacted by information risks, and how those risks might be managed. The SIRO is responsible for ensuring that information governance is embedded into the organisation to ensure that the potential risks to corporate information and records are mitigated. This is done by ensuring that policies and processes are in place for the safe management of information. The SIRO is supported in this role by the Corporate Governance Board and the Information Governance Steering Group. Duties include:

a) Taking ownership of the organisation’s information risk including escalation to the Corporate Risk Register
b) Acting as a champion for information risk at Corporate Governance Board
c) Providing written advice on the council’s statement of internal control regarding information risk as part of the Annual Governance Statement.

- **Data Protection Officer (DPO)**

Under the requirements of GDPR the Council is required to have a Data Protection Officer. The role provides independent advice to the council and is able to report directly to the Executive Board when required. The minimum tasks, as defined by GDPR are: -

    - To inform and advise the organisation and its employees about their obligations to comply with GDPR and other data protection laws
    - To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
    - To be the first point of contact for supervisory authorities and for individuals whose data is processed.

- **Monitoring Officer (MO)**
    - As the statutory officer in relation to the 'Access to Information[2]' rules, the MO determines whether reports, or parts of reports are 'exempt' or not for the purposes of Public Meetings run by the Democratic Services Team.
    - For advising on a councillors' entitlement to information.
    - Is responsible for determining, under FOIA whether exemption 36 (exemption from disclosure of information which might prevent the free and frank provision of advice or exchange of views; or otherwise prejudice the effective conduct of public affairs) can be relied on.

- **Executive Directors and Heads of Service**

are responsible for considering information management implications when planning to out-source services, work with partners or commission new technologies or major structural changes.

- **Information Asset Owners (Heads of Service)**

are accountable and responsible for ensuring appropriate information management practices are in place for their information assets (electronic and paper). Information assets can be defined as data, software, hardware, services etc.

- **Information Asset Managers (Managers/Team Leaders)**

are responsible for the day to day management of information and the risks of information used in their areas. Information Asset Managers are responsible for ensuring all information is retained on deleted in line with the Retention Schedule, likewise, ensuring it is up to date. Information Asset Managers are responsible for notifying the Data Protection Officer of any changes in processes that deal with personal data.

- **Information Governance (IG)Team**

are responsible for ensuring the council remains compliant with the legislations referred to in this Policy, managing security incidents and ensuring that training and awareness programmes are in place so that staff are aware of and understand their obligations.

- **Information Governance Champions (IGC)**

All Directorates have nominated Information Governance Champions who serve to represent all aspects of access to information within their functional area,

[2] Part VA of the Local Government Act 1972, as amended in part by the Local Government (Access to Information) Act 1985.

including Freedom of Information, Environmental Information Regulations and Data Protection. Meetings are held at least quarterly.

- **Line managers**

are responsible for ensuring that staff under their direction and control are aware of the policies, procedure and guidance relating to Information Governance and for checking that those staff understand and appropriately apply policies, procedures and guidance when carrying out their day to day work.

- **All staff, Councillors, contractors, partner organisations, consultants and agents** ("information users")

are responsible for managing information in accordance with this policy and related procedures. Upon leaving the Council all must ensure that key Council records for which they are responsible remain accessible. It is the responsibility of all information users to process information in accordance with Data Protection Legislation (GDPR and DPA2018) and be aware of how to deal with information requests under Freedom of Information Act, Environmental Information Regulations and requests relating to Individual's Rights (Data Subject Rights) as defined by the General Data Protection Regulation, adhering to the policies, procedures and guidance that are laid down by the Council for information governance and security.

13. Data Quality

The quality of information acquired and used within the Council is a key component to its effective use and management. As such, Information Asset Owners and managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

The Council has *adopted* the following data quality standards:

1. **Accuracy**: - our data shall be sufficiently accurate for its intended purposes, representing clearly and in sufficient detail the interaction provided at the point of activity. Accuracy is most likely to be secured if data is captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable the Council to make informed decisions at all levels. The need for accuracy must be balanced with the importance of the uses for the data, and the cost and effort of collection.
2. **Validity**: - data will be recorded and used in compliance with relevant requirements, including the correct application of any rules and definitions. This will ensure consistency between periods and with similar organisations. Data items held on Council systems and other record systems must be valid and contextually logical. Where possible free-text fields will be avoided, and standard codes or options used that comply with national standards or map to national values. Wherever possible computer systems will be programmed to only accept valid entries. In particular, steps will be taken to ensure that service-user details are validated for changes and accuracy throughout the duration of service provided by the Council.

3. **Reliability**: - our data will reflect stable and consistent data collection processes across collection points and over time, whether using manual or computer-based systems or a combination. Councillors, Managers and stakeholders should be confident that progress towards performance targets reflects real changes rather than variations in data collection methods.
4. **Timeliness**: - data will be captured as quickly as possible after the event and will be available for the intended use within a reasonable time period. Data must therefore be available quickly and frequently enough to support information needs and to influence both operational and strategic decision making. To that end, key staff, need to be aware of relevant deadlines.
5. **Relevance**: - data captured will be relevant for the purposes for which it is to be used. This will entail periodic review of requirements to reflect changing needs.
6. **Completeness**: - data requirements will be clearly specified based on the information needs of the Council, and data collection processes matched to these requirements. An assurance review may be instigated should monitoring identify missing, incomplete or invalid records. In this respect the assurance and feedback processes will be adhered to, ensuring quality of data.
7. **Documented Procedures**: - in order to minimise errors and achieve good quality data, appropriate procedures and guidance must exist so that staff can be trained and supported in their work. Details of these procedures, processes and training will be contained in any relevant manuals and available to all staff.

14. Records Management

Information Lifecycle (Appendix 1). Records must be managed through their lifecycle; from creation, through storage and use, to disposal

14.1. Creation and maintenance

14.1.1. Information ***users*** will:

- Create, keep and manage records which document the Council's principal activities.
- Maintain records that the Council requires for business, regulatory, legal and accountability purposes. The requirements for different classes of records are documented in the corporate Retention Schedule.
- Create records with meaningful titles and indexes/metadata so that they can be retrieved quickly and efficiently.
- Make sure records are authentic, reliable, have integrity and remain usable. This includes making appropriate arrangements for ensuring the continuity and availability of information when staff leave, or during major organisational or technological change.

14.1.2. Information ***asset owners*** will:

- Ensure appropriate business continuity arrangements are in place for all records both electronic and paper

14.2. Storage

To maximise efficiency, reduce costs, enable sharing and minimise risks information users will:

- Store key business information in **shared** corporate repositories (e.g. J drive, Kahootz, GIS etc.)
- Store information **securely**, appropriate to its classification
- Avoid storing duplicates (e.g. avoid paper/electronic overlaps, e.g. store a single copy of electronic information to be shared through use of links) and **routinely destroy temporary material.**
- Not store information permanently on **removable media.**

14.3. Commissioners and Information asset owners will:

Make appropriate **contractual arrangements** where information is stored, managed or hosted elsewhere on behalf of the council.

14.4. Use

In order to balance the Council's commitment to openness and transparency and a desire to exploit our information with responsibility for privacy and sensitivity requirements, information users will:

- Ensure all Council records are subject to appropriate security measures as set out in our Information Security policy and related policies.
- Document decisions regarding access so that they are consistent and can be explained and referred to.
- Proactively publish information where it is considered, by the team, Governance and Information Manager, and/or Legal Team to be in the public interest.

14.5. Disposal and Retention

14.5.1. The Information Governance Manager will:

Publish and promote, using relevant communications methods, the Council's records retention schedule so that staff are aware of which records the Council has decided to keep and their personal responsibility to follow the retention schedules.

14.5.2. Information Users will:

- Review records in accordance with the retention schedule when they are no longer required for on-going business or specific legal or regulatory purposes.
- Review records at the end of their retention period and arrange for secure destruction or in certain circumstances give a further review date.

Documentation of the disposal or transfer of records will be completed and retained.

- Manage electronic records in accordance with the corporate retention schedule. We will not preserve everything. All new computer systems must be GDPR compliant. It is recommended that an intended disposal or review date is captured when creating electronic records
- Ensure records subject to active/live requests under Freedom of Information, Environmental Information Regulations or Data Protection are not destroyed.

15. The Strategy

Effective Information Governance Management will be achieved through the following methods: -

15.1. Mandatory Training and Awareness

Fundamental to the success of delivering a robust Information Governance agenda across the Council is the development of an Information Governance awareness culture. Training will be provided to all staff to promote this ethos. In addition to formal Information Governance training, a layered approach to awareness is employed, acknowledging a broader understanding of training to encapsulate awareness raising. Some roles, such as SIRO and IAOs are required to undertake regular training to remain current in their role.

15.2. Confidentiality Code of Conduct

All staff must be aware of their individual responsibilities for the maintenance of confidentiality, data protection, Information Security management and data quality. They are given the tools for this through annual mandatory Information Governance training, annual review of the Information Governance Strategy and Framework and the Information Governance Handbook. All new staff will be made aware of the Handbook as part of their Data Protection and Cyber Security e-learning and all staff are annually directed to it in the Information Governance Staff Handbook.
It is made clear in both in both the Information Governance training and documentation that failure to maintain confidentiality may lead to disciplinary action, including dismissal.

15.3. Communicating Confidentiality and Data Protection

The Information Governance and Digital Design Teams maintain an Information Governance and Information Security Improvement Plan. This includes actions to ensure that residents and the public are adequately informed about confidentiality and the way their information is used and shared.

15.4. Information Asset Management and Business Continuity

A core Information Governance objective is that Information Assets (systems) and the use of information in them are identified and that the business importance of those assets is established.

Information Assets are those that are central to the efficient running of the Council and specific teams, e.g. Housing Benefit, Council Tax, Planning, HR, Finance etc. They also include, but are not limited to the following examples:

- **Information** – system documentation and procedures, archive media and data.
- **Software** – databases, application programs, systems, development tools and utilities.
- **Physical** – infrastructure, equipment, furniture and accommodation used for data processing.
- **Services** – computing and communications, heating, lighting, power, air conditioning used for data processing.
- **People** – qualifications, skills and experience in the use of information systems.
- **Intangible** – the Councils reputation.

Essentially, it is information in any format that is of value to the organisation and would be problematic if it were not accessible.
The Council has clear lines of accountability for Information Risk Management (IRM) that lead directly to the Board through the SIRO (see Appendix 2).
Information Asset Owners (Heads of Service) are the nominated owner for one or more of the Councils identified Information Assets, and report for this function to the SIRO. There is detailed guidance available for Information Asset Owners and Managers.
Whereas it is ideal that all assets are clearly identified on the Information Asset Register, the Council has a risk-based approach that gives priority to Information Assets that comprise or contain Personal Confidential Data[3] and / or would have the greatest impact on customers, staff, a particular team and/or the Council if they were not available.
The SIRO has the final decision on approving identified risk mitigation plans. Serious risks must be entered onto the Corporate Risk Register for Board consideration.
All changes to Information Assets, such as system upgrades, should follow an established change control procedure, such as a Data Protection Impact Assessment (formerly known as a Privacy Impact Assessment, see Section 17 below).

When considering transferring Personal Confidential Data outside of the UK there is a requirement under data protection legislation to ensure there is a legitimate basis for doing so when those jurisdictions do not have adequate DP regulation, as this ensures Data Subjects information is not undermined. The DPO should be consulted on every occasion.

[3] See Staff IG Handbook for more detail

16. Information Risk Management

The Council is committed to making the best use of the information it holds to provide efficient services to its customers and the local economy while ensuring that adequate safeguards are in place to keep information secure and to protect Data Subjects' right to privacy.

The council recognises that information handling represents a significant corporate risk in that failures to protect information properly or use it appropriately can have a damaging impact on its reputation. Furthermore, failure to protect information adequately can attract the attention of the Information Commissioner's Office (ICO), which regulates Freedom of Information, Environmental Information Regulation and Data Protection legislation and has access to a range of sanctions including the significant fines.

Information risk management complements the Council's risk management framework. As part of this, information risks are clearly recognised, and the appropriate controls implemented through a Board approved corporate risk management strategy and policy.

Information risk is intrinsic in all administrative and business activities and all staff must continuously manage it. The council recognises that the aim of Information risk management is not to eliminate risk, but to provide the structural means to manage it, by balancing its treatments with anticipated benefits that maybe derived.

The council acknowledges that Information risk management is an essential element of broader Information Governance and Information Security arrangements and is an integral part of good management practice; it should not be seen as an additional requirement.

The risk management framework is dependent on allocating clear organisational responsibilities, identifying all the Information Assets, assessing the associated risks and managing any incidents arising from them.

This will:

- Protect the council, its staff and its customers from information risks where the likelihood of occurrence and the impact is significant.
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
- Encourage proactive rather than reactive risk management.
- Inform decision making throughout the council.
- Meet legal and statutory requirements.
- Assist in safeguarding the council's Information Assets.

Information Risk Assessments are performed for all information systems and critical Information Assets at the following times:

- Ahead of introducing new systems, applications, facilities, etc. that may impact the assurance of Council information or systems, a Data Protection Impact Assessment (DPIA) will be carried out (see section 17 below).

- Ahead of agreeing enhancements, upgrades, and conversions associated with critical systems or applications. Those containing, or which involve personal information will also require a DPIA.
- When Council policy, legislation or associated guidance requires risk determination, or when that legislation and guidance is changed or updated.
- When required by the Council, as directed by the SIRO, or Information Governance Manager / Data Protection Officer.

As in the Council's overarching Risk Management Framework, any Risk Assessments scoring 16 or above must be entered onto the Corporate Risk Register. Every attempt should be taken to Treat, Mitigate or Eliminate risks scored as anything other than Green on the scoring matrix. Any scoring Red will be considered by the SIRO for addition to the Corporate Risk Register. The DPIA process is intentionally designed to ensure all new / amended processes are introduced with the least possible risk apparent.

Information incident reporting is in line with the Councils overall information security reporting Indicators that information risk management is being positively enacted include but are not limited to successful Internal Audits of Information Governance, Data Protection and Information Security and there having been no involvement from the ICO as a result of significant data protection breaches or data subject rights complaints.

Alternate yearly reviews will be carried out by the IG Team on behalf of the SIRO and reported to Information Governance Steering Group or other suitable management route. Overall responsibility for action plans lies with the SIRO, to be completed by relevant Information Asset Owner and monitored by Information Governance Steering Group.

16.1 Associated Risks

There is a risk to the Council in not complying with the legal, regulatory and statutory obligations, best practice, internal and external controls if Information Governance arrangements are not managed and reported effectively.
There is also a graded risk to the Council in not complying, resulting in potential adverse publicity and the consequent impact on Council's reputation.

These could be categorised as:

- Insignificant – Potential for public concern
- Minor – Local media coverage, short term reduction in public confidence
- (elements of public expectation not being met)
- Moderate – Local media coverage, long term reduction in public
- confidence
- Major – National media coverage – service well below reasonable public
- expectation
- Catastrophic – As above, with questions raised in the House of Commons, resulting in potential total loss in public confidence.

17. Data Protection Impact Assessments (DPIA)

In line with ICOs guidance, a DPIA must be undertaken for any project, procurement, business case, transfer of Personal Data or departmental / team initiative where there is a potential impact upon the privacy of individuals.

DPIAs are a Risk Assessment tool to analyse how a project or system will affect the privacy of the individuals involved. Projects are not formally defined by the Council but must be understood to be any plan or proposal, including potentially any procurement, business case and / or departmental / team initiative that include transfers of Personal Data and / or potential sensitive business information.

The DPIA process must be an integral to conventional project management techniques and be started from the very earliest stages of the project's initiation, often as a result of a business case process being invoked.
DPIAs are chiefly concerned with an individual's ability to manage their information; the Council's processes are therefore aligned to data protection, with specific concentration being given to the minimising of harm arising from intrusion into privacy, as defined by those principles.

An effective DPIA allows the organisation to identify and resolve any such problems at an early stage, minimising costs and reputational damage which might otherwise occur. The Information Governance Team are responsible for maintaining the DPIA register and working with teams on completion of the assessments

Directors, Managers and Team Leaders at all levels, and Information Asset Owners must ensure that all existing contracts are monitored and reviewed half yearly to ensure that Information Governance controls are being adhered to and to resolve problems or unforeseen events.
A Register for all third-party contracts is held centrally by the service responsible for the contract

18. Information Sharing

Sharing and use of information about individuals between teams and/or between partner agencies is vital to the provisions of co-ordinated and seamless provision of Services. The Council recognises the need for shared information and robust information security to support the implementation of joint working arrangements.

18.1. Information/Data Sharing Agreements

Are essential, not only do they provide transparency for all parties needing to share information but also provides assurance in respect of the standards that each party agrees to adopt. A sharing agreement is required for both **large-scale regular / permanent** sharing, such as giving access to a particular system. The Information Governance Team have a template teams can use and keep a register of sharing agreements. The Data Protection Officer can provide advice on data sharing agreements to ensure data protection considerations have been met and the sharing is compliant with data protection legislation.

18.2. Disclosure of Information to the Police and other Organisations

Under the Law, no organisation has an automatic right to see personal data about customers or staff. When requests are received, they are considered individually on their own merit and personal data is not released without careful consideration. All requests for Council information must go through the Data Protection Officer to ensure the request meets the exemption under data protection legislation.

19. Information in Transit

Whether individuals are taking paper files out for site visits, meetings etc or sending information electronically or physically all staff should be aware of protocols to use. For example, the haven protocols if sending confidential information (personal or otherwise) by fax. If sending electronically then personal/sensitive data should be contained within in a password protected document e.g. word or excel. If using Royal Mail then think about whether 'recorded', 'signed for' or 'guaranteed' should be used. More information can be found in the Staff Information Governance Handbook. Managers/Team Leaders are responsible for providing guidance to their staff on taking physical information out of the office environment.

20. Information Governance, Information Security and Cyber Security Incidents

ISO 270001, the International Standard on Information Security defines the concept as the 'Preservation of confidentiality, integrity and availability of information', adding that other properties are involved, such as authenticity, accountability, non-repudiation and reliability.
Increasingly all organisations and their information systems and networks are faced with security threats from a wide range of sources, including lost or stolen equipment or data, computer-assisted fraud, sabotage, vandalism, fire or flood.

To prevent unauthorised access to information systems, formal procedures are in place to control the allocation of access rights to information systems and services and cover all stages in the lifecycle of system access. This is supported by the Information Asset Owner/Manager process outlined above.

Users are made aware of their responsibilities for maintaining effective access controls through the inclusion of Information Governance and Data Protection and Cyber Security training, particularly with regard to the use of passwords and the security of equipment. In addition, the Council has signed up to the National Data Security Standards whilst directly applicable to the NHS they can likewise be applied to all organisations. The security standards can be found at Appendix 3.

The Data Incident reporting procedure[4] must be followed when an incident occurs.

[4] Under Review

Examples of, but are not limited to:

- Lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Disclosed in error
- Uploaded to website in error
- Non-secure disposal – hardware
- Non-secure disposal – paperwork
- Technical security failing (including hacking)
- Unauthorised access/disclosure

On receiving notification of a potential serious incident requiring investigation, the Information Governance Team must inform the SIRO, or in their absence a Director/Chief Executive and the relevant Head of Service as soon as practicably possible to seek advice and guidance, as appropriate.

The decision to report externally to the ICO, lies ultimately with the SIRO, based on the advice of colleagues such as the relevant Head of Service and Data Protection Officer.

Information Governance Steering Group has a key function to monitor and review Information Governance incident trends and guide overarching remedial action to those trends.

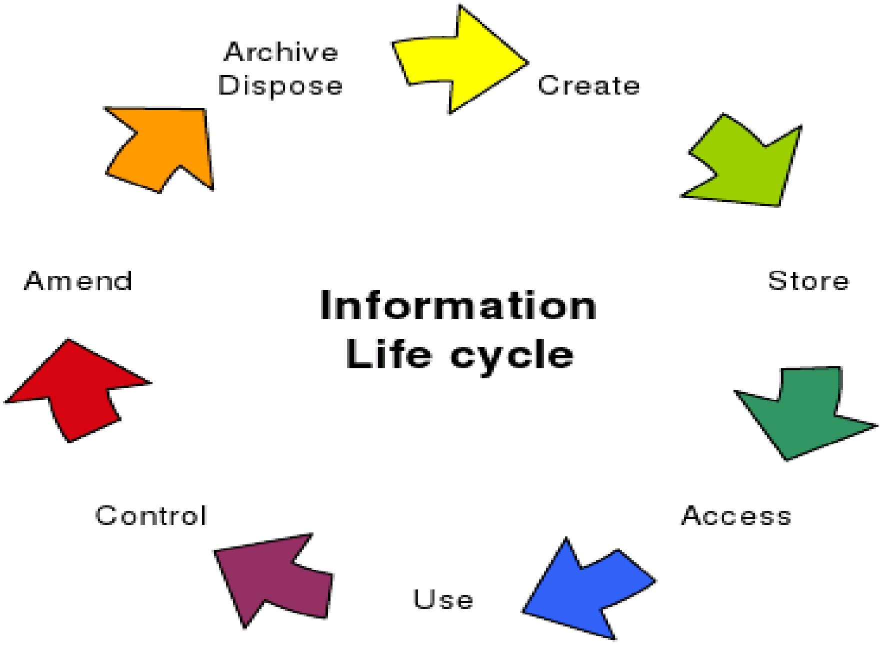
21. Monitoring compliance with, and the effectiveness of, the Information Governance Strategy and Framework

Monitoring and review:
This is a medium term, 3-year strategy, the work programme can be found at Appendix 4. The aims are supported by an Action Plan (Appendix 5) with key actions reinforced through Service Plans. The implementation and success of the Strategy and the Action Plan will be monitored quarterly by the Information Governance Steering Group and reported through to the Corporate Governance Board.

Policies, procedures, standards and advice are available to staff at any time on the Information Management pages. There will be an annual review of the information management work programme by the Information Governance Steering Group to determine the progress made in completing the actions. As part of this review and where appropriate, the priority level for implementation will be amended and any work that is deemed as complete will be removed from the programme.

Compliance with this document will be monitored through its associated policies and relevant sections within the Council's Constitution

Appendix 1 - Information Lifecycle:



Create	As soon as you start typing or writing you are creating a document and your responsibility starts here for its security and management
Store	Once you plan to save your document you need to think about who needs access, where it should be stored.
Access	Access can change during the lifetime of a document. From being the first draft of a Royal visit or Olympic torch relay where there are security implications and information is tightly controlled through to publishing to outside authorities, the public and media.
Use	How will this be used? Is it a working document like a spreadsheet or does it record a decision like minutes or a contract? If it's lost, destroyed or damaged how much impact would it have on the Council? Do you need to share it with another team or organisation? Do you have the authority or a data sharing agreement in place?
Control	All employees who have access to the information are responsible for its safe keeping. Ensuring that if it's shared it is done so where there is a clear business need and all data protection rights are handled correctly. Additionally, each team must have an Information Asset Owner (Head of Service) and Information Asset Manager (Manager/Team Leader) whose job it is to at least annually review access rights, data sharing, security, retention, data protection, risk assess the information and help review if there are any reported breaches.
Amend	If information is updated where appropriate use version control. This limits the chance that were information is shared old versions are accessed in error.
Archive/ Disposal	Destruction and archiving is in line with the Council's Retention Schedule unless the information forms part of an ongoing information request (FOI/EIR or DP), Local Government Ombudsman Complaint or legal action. If in doubt, ask the IG Team.

Appendix 2 – National Data Security Standards

Whilst relevant to the NHS, still valid for all Public Authorities

Leadership Obligation 1:
People: *Ensure staff are equipped to handle information respectfully and safely*

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2. All staff understand their responsibilities under data protection legislation including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. All staff complete appropriate annual data security training.

Leadership Obligation 2:
Process: *Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.*

4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6. Cyber-attacks against services are identified and resisted and Capita security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

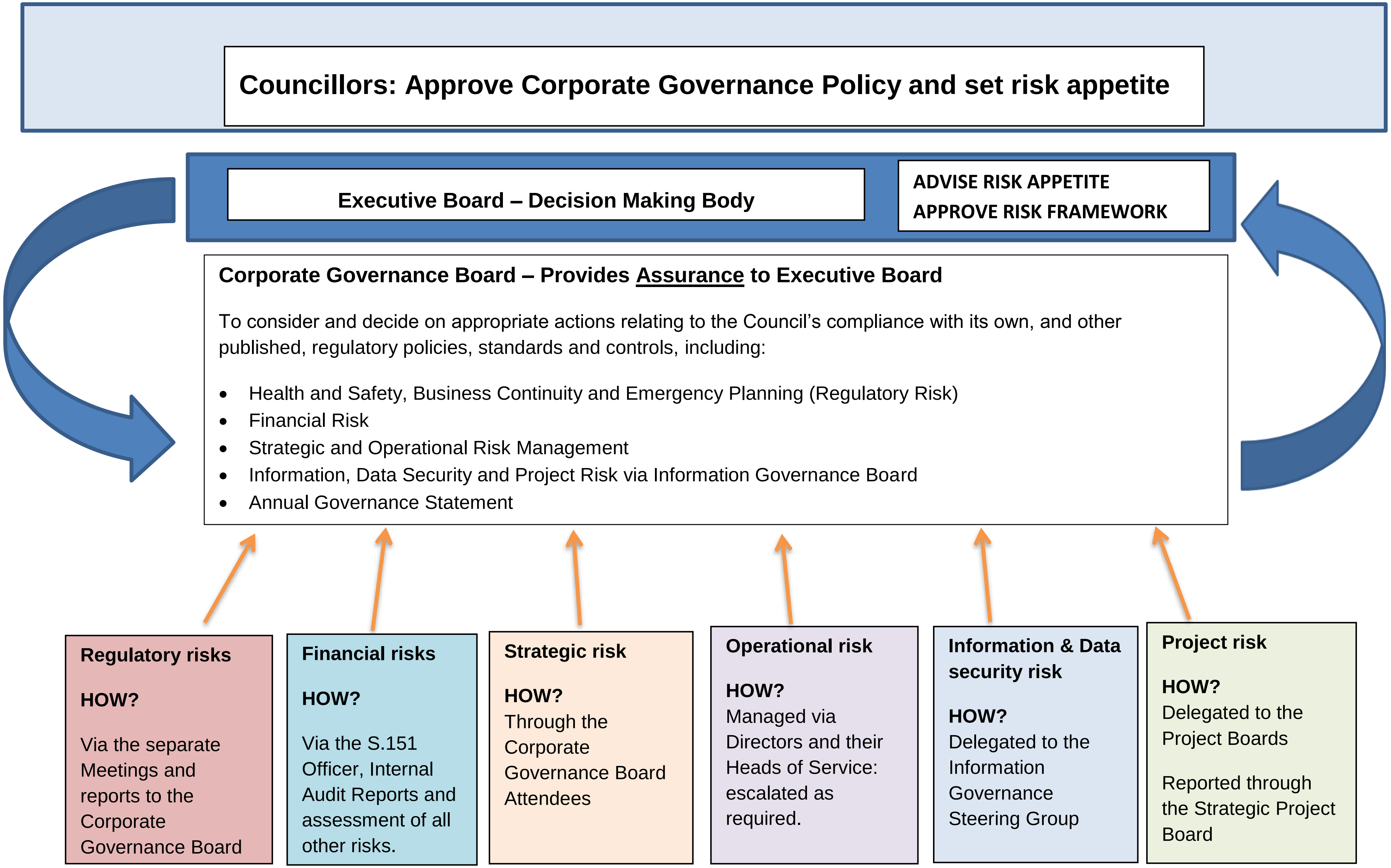
Leadership Obligation 3:
Technology: Ensure technology is secure and up-to-date.

8. No unsupported operating systems, software or internet browsers are used within the IT estate.

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting data protection legislation principles.

Appendix 3 - Corporate Governance Model



Councillors: Approve Corporate Governance Policy and set risk appetite

Executive Board – Decision Making Body

ADVISE RISK APPETITE

APPROVE RISK FRAMEWORK

Corporate Governance Board – Provides Assurance to Executive Board

To consider and decide on appropriate actions relating to the Council's compliance with its own, and other published, regulatory policies, standards and controls, including:

- Health and Safety, Business Continuity and Emergency Planning (Regulatory Risk)
- Financial Risk
- Strategic and Operational Risk Management
- Information, Data Security and Project Risk via Information Governance Board
- Annual Governance Statement

Regulatory risks

HOW?

Via the separate Meetings and reports to the Corporate Governance Board

Financial risks

HOW?

Via the S.151 Officer, Internal Audit Reports and assessment of all other risks.

Strategic risk

HOW?
Through the Corporate Governance Board Attendees

Operational risk

HOW?
Managed via Directors and their Heads of Service: escalated as required.

Information & Data security risk

HOW?
Delegated to the Information Governance Steering Group

Project risk

HOW?
Delegated to the Project Boards

Reported through the Strategic Project Board

Appendix 4 - Information Management Strategy - Work Programme 2018-2021

The Information Management Strategy Work Programme details the actions required to ensure the Council’s aims for information management are being achieved. The programme includes actions that are already fully implemented but require continual review or are partially implemented and they have been prioritised as ‘ongoing’. There are actions that have been given a priority as 1, 2 or 3.

The Work Programme is split into two tables –the actions with a priority of 1, 2 or 3 are detailed in the first table and ongoing actions are detailed in the second table. This allows effective monitoring of actions to take place.

Action Plan – Actions identified as priority 1, 2 or 3

Priority:

1 = to be achieved as a priority

2 = to be achieved as a medium-term priority

3 = to be achieved as and when resources are available

Ref.	Objective	Actions	Priority	Progress	Responsible officer
Aim 1: Access to information					
1.1	To build a new Intranet	Review/audit current Intranet (Skoop) content, to identify develop requirements and migration volumes	2	Currently in audit phase	Digital Designer – Information Solutions
1.2		Enhance ‘Search’ functionality, to improve site efficiency	2		Digital Designer – Information Solutions
1.3	Data Audit J: Drive	Identify/confirm data owners for all Corporate Network folders	2	Currently in audit phase, identifying Information Asset Owners	Digital Designer – Information Solutions
1.4		Review/audit folders to identify and resolve duplicate/obsolete/non-compliant data	2	Currently in audit phase, identifying Information Asset Owners	Digital Designer – Information Solutions
1.5		Review network folder structure	2	Currently in audit phase, identifying Information Asset Owners	Digital Designer – Information Solutions

Ref.	Objective	Actions	Priority	Progress	Responsible officer
1.6	To maintain a well organised electronic network drive.	Each department to develop a plan for the arrangement of their electronic network drive to enable it to un-duplicate and clean their existing network drive file stores.	2	Dependent on Aim 1.2	Digital Designer – Information Solutions
		Implement the plan (above).	2	Dependent on Aim 1.2	Digital Designer – Information Solutions
	To publish all mandatory information as required under the Local Government Transparency Code 2015.	All relevant departments publish their own information as prescribed by the 2015 Code and to ensure publication in accordance with mandatory timescales.	1	Last checked January 2019	Information Governance Manager
Aim 2: Efficient and effective management of Information					
2.1	To carry out audit of existing policies	Identify areas where there are gaps and/or policies, standards/procedures are required	1	Links to Corporate Initiative	Information Governance Manager
2.2	To ensure relevant staff are aware of Records Management Best Practice	Development of a specific Records Management Procedure.	2	Records Management Training identified, dates to be confirmed	Information Governance Manager
		Launch and raise awareness of records management to appropriate staff.	2	Once training undertaken workplan can be devised and rolled out	Information Governance Manager
2.3	To ensure consistent use of the policy document template which have a cover page and version history table to enable tracking of changes	Review existing policies to establish whether they have a cover page and version history table in accordance with the template and update as necessary.	1	Communications team have document template. Existing and new policies to be rolled out in line with corporate template	Information Governance Manager

Ref.	Objective	Actions	Priority	Progress	Responsible officer
	through the document's active life.	Communicate the template for use across the Council.	2	Once constitution review has been completed, Democratic Services Manager to ensure appropriate template is used.	Information Governance Manager
2.4	To have secure destruction of confidential Information.	To review the current process and act as necessary to ensure that all confidential information is disposed of securely.	2	Communications Plan using Culture Change Champions	Information Governance Manager
		Ongoing: To ensure all electronic equipment is cleared of information before disposal. Equipment Disposal 'form' is completed to record risk assessment	2	Management Process to be documented	Digital Design Team Leader
2.5	To have a current asset registers in place	Identify and register all council assets including mobile devices into 1 register	2	Work with Capita to identify all council assets	Digital Design Team Leader
		To have a defined and maintained Information Asset Register (IAR)	2	Identify gaps in existing IAR	Digital Designer – Information Solutions
2.6	To have an appropriate Information Protection and Disaster Recovery Plan.	Undertake a risk assessment into how the Council's physical information is stored, preserved and protected from the fire, flood, theft and loss.	2	Areas identified, management plan to be created	Safety and Emergency Planning Officer / IG Officer
2.7	To review and update the Councils Retention Schedule on periodic basis	Team level understanding of their responsibility in developing the council's retention schedule	2	Continue to communicate to Information Asset Owners and Managers their role in retention	Information Governance Manager

Ref.	Objective	Actions	Priority	Progress	Responsible officer
Aim 3: Staff with appropriate skills in dealing with information					
3.1	Increase staff awareness of information management, security and data protection.	Establish the Information Governance delivery of training using e-learning, IG Framework and IG Staff Handbook	1	Communications plan for roll out of Policy and Strategy, IG Staff Handbook and subsequent IG Training.	Information Governance Manager
3.2		Monitor staff attendance on mandatory training courses each quarter.	1	Quarterly updates provided to the Information Governance Steering Group	Information Governance Manager
3.3		Data Protection updates: Ensure refresher training is diarised annually after undertaking initial e-learning training.	1	Quarterly updates provided to the Information Governance Steering Group	Information Governance Manager
3.4	Ensure the council has the Digital Tools to secure council's data	To review the digital controls available to assist users	2	To ensure the 3 streams of the workstyle review take account of availability digital controls	Digital Design Team Leader
Aim 4: Appropriate Information Sharing					
4.1	Have clear and relevant Information Sharing Protocols in place and raise staff awareness of these.	Create a central register of Information/Data Sharing Agreements. Work with services to identify where agreements are in place	1	Register in place; Engagement with services to implement	Information Governance Manager
4.2		Communicate guidance on Information Sharing and promote the existing template protocols to staff to raise awareness.	2	Communications plan required	Information Governance Manager

Ref.	Objective	Actions	Priority	Progress	Responsible officer
4.3	Information Asset Owners and Managers / Legal team aware of GDPR implications for contracts	GDPR requirement to have Information Sharing Agreements in place when contracts contain personal and/or special categories data.	1	IG solicitor to lead on from Legal perspective and on-going communications to Information Asset Owners/Managers	Information Governance Manager
Aim 5: Information Security					
5.1	To have in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data	All relevant Information Security policies are to be reviewed in accordance with frequency included in the Information Policy Register (Appendix 6).	3	Majority of 5 Councils agreed policies have been approved and going through Councils formal approval and adoption route	Information Governance Manager
5.2		As part of the existing review process, all relevant information security policies and procedures are revised (where appropriate) to consider legislation, changes in existing policy and mandatory requirements.	3	As policies require approval the relevant service(s) will be involved for any legislative or other amendments.	Information Governance Manager
5.3		Information security policies and procedures are communicated to staff in a layered approach utilising communications team	2	Communications Plan for staff	Information Governance Manager
5.4		Ensure the council has the Digital Tools to secure council's data on both Council assets and BYOD i.e. 2FA and MDM	2	Ensure all staff are aware of their responsibilities whilst digital tools are being investigated	Digital Design Team Leader

Ref.	Objective	Actions	Priority	Progress	Responsible officer
Aim 6: Councillors Engagement with Information Governance					
6.1	All Councillors participate in training available for staff	Ensure appropriate training is made available and provide advice and awareness for all Councillors	2	Information Governance Training to be rolled out to Councillors as part of the Councillor Training Programme	Information Governance Manager

Appendix 5 - Work programme for ongoing actions

Ref	Objective	Actions	Responsible officer
Aim 1: Access to information			
1.1	To maintain a central repository of all policies and guidance relevant to information management so that staff and members can easily access them.	The Policy Hub is a central repository for all policies. There are links from the Information Management tab on the Intranet	Information Governance Manager
1.2	To maintain a list of the information assets.	The Information Asset Register is in place and is reviewed every year.	Information Owners
1.3	To maintain a register of processing activity (ROPA)	The ROPA is in place and is reviewed every year.	Information Governance Manager
Aim 2: Efficient and effective management of information			
2.1	To ensure policies relating to information management are subject to an appropriate review cycle.	Maintenance of the Information Policy Register (Appendix 3) and to undertake policy reviews undertaken when required.	Information Governance Manager
Aim 3: Staff with appropriate skills in dealing with information			
3.1	Increase staff awareness of information management and security	Existing information management and security policies are communicated to all members of staff on a regular basis.	Information Governance Manager
		Information Governance and Security training is incorporated into the induction process.	Information Governance Manager
		Data Protection and Cyber Security E-learning: Ensure refresher training annually	Information Governance Manager
3.2	Continue to raise staff awareness of FOI/EIR and access to records under the GDPR and other data protection law obligations.	FOI/EIR and DP training is incorporated in the induction process.	Information Governance Manager
3.3		There are Information champions within each Service liaising with the IG Team on IG Matters e.g. Access to Information, Retention etc.	Information Asset Owners
Aim 4: Appropriate information sharing			
4.1	Have clear and relevant Information Sharing Protocols in	Exercise previously undertaken to: Identify where information sharing takes place.	Information Governance Manager

	place and raise staff awareness of these.	Where information sharing takes place, a protocol is developed if one did not already exist. Review existing protocols on a regular basis.	
		Information Sharing is covered on the Information Management Tab on Intranet and contains all guidance on information sharing.	Information Governance Manager
4.2	To have appropriate measures in place to enable the Council to share information as required by Government Connect.	Meeting the appropriate requirements in the Code of Connection (PSN) on an annual basis.	Digital Design Team Leader
Aim 5: Information security			
5.2	To have secure links to the Government Connect Secure Extranet	Meeting the requirements as set out in the Code of Connection (PSN). Meeting the requirements for cyber security standards.	Digital Design Team Leader

Appendix 6 - Internal Policies

Policies, which include guidelines and procedures, are located on the Council's intranet (SKOOP) Information Management Tab.

Policy	Next Review date	Approver
RETENTION AND DESTRUCTION		
Register of Processing Activity (living document)	October 2020	Information Asset Owners
INFORMATION SECURITY		
Security Incident Management & Cyber Response Policy	July 2020	Corporate Governance Board
IT User Policy	February 2020	Corporate Governance Board
Acceptable Use Policy	April 2020	Corporate Governance Board
Email Policy	February 2020	Corporate Governance Board
Password Policy	April 2020	Corporate Governance Board
Remote Access Policy	July 2020	Corporate Governance Board
Removeable Media Policy	February 2020	Corporate Governance Board
Risk Management Policy	February 2020	Corporate Governance Board
Software Policy	July 2020	Corporate Governance Board
Mobile Device Policy	August 2020	Corporate Governance Board
Mobile Phone Policy	June 2020	Joint HR Committee
Information Security Statement	November 2020	Corporate Governance Board
INFORMATION GOVERNANCE POLICY, STRATEGY AND FRAMEWORK		
Information Governance Policy, Strategy and Framework	September 2020	Corporate Governance Board