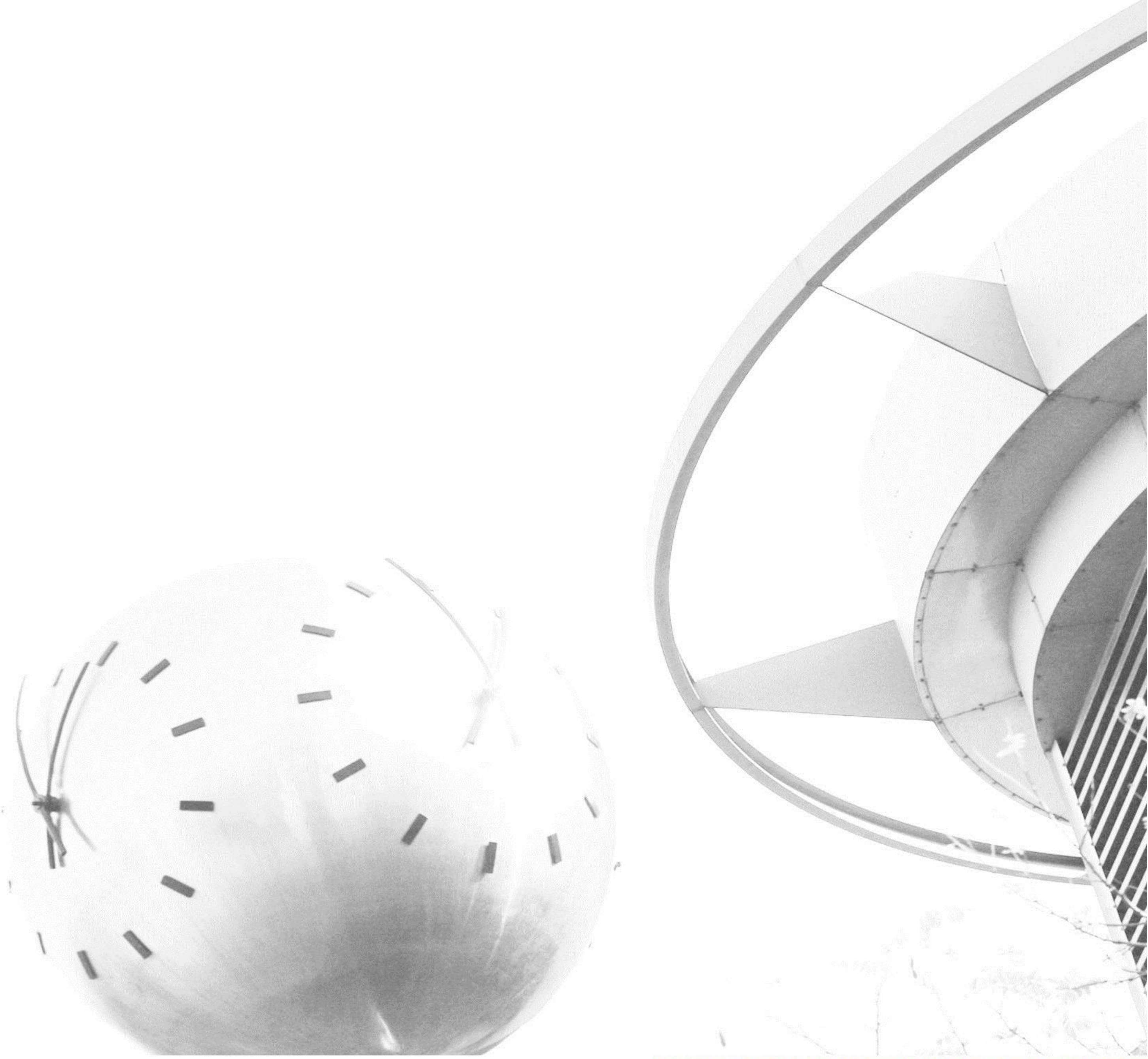
ENCLOSURE NO. 2

Information Management Policy

2021-24



BasildonCouncil
BASILDON • BILLERICAY • WICKFORD

Creating Opportunity, Improving Lives

Key Information

Author:	Omolade Oshunremi
Section/Directorate:	ICT
Service Impact Assessment:	Approved
External Consultation:	N/A
Internal Consultation:	Information Governance Working Group Key officers involved in development of Policy throughout process
Background Information:	Information Principles for the UK Public Sector, HM Government Information Sharing Protocols, ICO Whole Essex Information Sharing Framework
Policy Approval – Officer Level	Stuart Young Director of People and Change
Policy Approval – Member Level	Policy Executive Committee

Compliance
All staff, members and contractors or others with access to Council's information must comply with this policy. Anyone who is found to have breached this policy could be subject to Basildon Borough Council's Disciplinary Procedure and The Code of Conduct and serious breaches of this policy could be regarded as gross misconduct. If you do not understand the implications of this or how to apply it in your day to day working practice, seek advice from Human Resources.

Advice and Training
If you do not understand anything in this policy or feel you need specific training to comply with it, you should bring this to the attention of your line manager. The Information and Compliance Manager or Data Protection Officer can also provide further advice and guidance in respect of this policy

Content

1. Introduction

Basildon Council holds and processes a range of information about the people, places, events, and businesses of the Borough, including staff who work with and on behalf of the Council. This information enters the Council from a variety of sources, including from other partner agencies. Essentially, the council cannot provide services to its residents and stakeholders without the collection, use, and disposal of information.

This policy recognises information and data as an intrinsic and valuable asset to the Council. It can provide knowledge and evidence which in turn can be used to inform Council policy and decision-making. Additionally, the ability for the organisation to meet and deliver the needs of the Borough in the future will depend increasingly on how well information is managed and how effectively it is used. For this reason, a robust structure of policies, protocols and procedures underpin this policy and are necessary to reflect the value of this asset, with the aim that it continues to be viewed in high regard across all departments, services and customers alike.

An effective policy should set out a clear rationale for the collection, processing, and destruction of information and the governance requirements necessary to ensure;

a) Information is fit for purpose
b) Information is re-use (record once, use many times)
c) Information is standardised and linkable

Adopting a clear framework is vital to facilitate the successful sharing of information, both internally and externally, as well as the appropriate processes for the management of data. Additionally, this framework will lay the foundations for our information management practices to be transformed or expanded, as necessary.

2. Executive Summary

Information management and governance is an essential component of organisations across all sectors. Data protection laws implemented in 2018 have been key drivers in developing an updated, rigorous policy to guide the organisation in the management of the information it collects and processes. The Data Protection Act 2018 has given individuals greater control over their personal data, whilst also promoting principles and safeguards that the Council will implement and promote. Moreover, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Local Government Transparency Code 2015 provide regulations allowing public access to information held by public authorities and set out the minimum data that local authorities should be publishing, as well as guidelines for this.

Basildon Council is committed to the implementation of good information management practice. This will help ensure that data is consistent and appropriately confidential, whilst also maintaining integrity and availability of data across all levels of the workforce. Appropriate guidelines and training will be available for all officers regarding the management of both physical and electronic information assets held by Basildon Council, in line with the requirements of this policy.

3. Scope

This policy applies to all Elected Members, Staff, Contractors and voluntary bodies accessing or receiving Basildon Borough Council data and information systems.

4. Policy Statement

The council recognises the importance of information as an asset, the need for effective records management, and respects the information rights of the individual. Basildon Council will collect, share, and utilise relevant, minimum, and appropriate information in a safe, lawful, and consensual way, in line with national legislation. It will ensure shared responsibility across the organisation to manage information correctly, thereby safeguarding our customers' rights and ensuring a valuable corporate asset is utilised effectively.

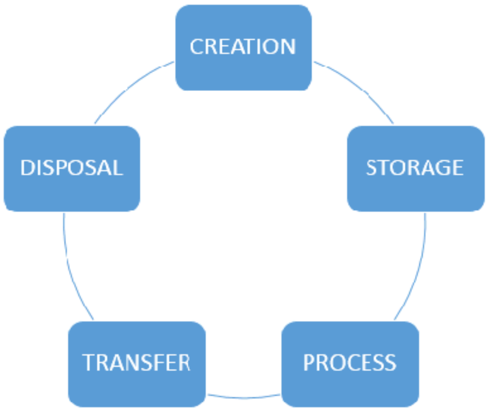
5. Information Management

Basildon Council's approach to information management and data handling provides the guiding principles and assurances necessary to fulfil the activity of information management, as well as the promotion of the positive use of information that we collect and store as an organisation. Supporting codes of practice, procedures and guidelines provide further details and establish the Information Management framework, which will sit beneath this policy document.

Information Management Lifecycle

The Council will commit to good information management practices by following the five steps of information life cycle model.

The Information Life Cycle



5.1 Creation

We will only collect the minimum data set necessary to fulfil our legal, statutory and business objectives.

5.2 Storage

We will store electronic data in a secure manner using state of the art information technology. Sensitive personal data will be protected using appropriate encryption techniques to ensure its continued confidentiality, integrity and availability (CIA).

Personal data shall be stored in line with the Council Information Architecture to facilitate the easy and complete recovery of personal data required to satisfy all data subject rights in line with the Data Protection Act 2018. Paper documents shall be stored in dedicated File Storage boxes and clearly identifiable with the owner and retention period appended to the front of the box;

5.3 Process

Document and data creators are responsible for ensuring data is accurate, relevant and up-to-date. Information will be recorded once and used many times. Where technology permits, routine business processes will be automated to maximise business efficiency;

5.4 Transfer

Electronic data transferred outside of the Councils IT network will be recorded in the Register of Processing Activities in accordance with article 30 of the Data Protection Act 2018. Where required, data encryption will be used to ensure all transfers of personal information are secure. All transfers of personal information will have the appropriate data sharing or data processing agreements in place prior to the commencement of any data transfer;

5.5 Disposal

All electronic data stored on the Councils ICT systems will be subject to the retention periods prescribed in the Corporate Retention Schedule. Non-application based data stored in the cloud (M365) will be subject to an automated data destruction process. This process ensures that data will be securely destroyed at the end of its useful life with the minimum staff intervention.

Paper records will be subject to retention and stored in records management boxes which clearly record the content, owner and disposal date on the front of the box. All documentation shall be securely disposed of on reaching the file destruction date.

6. Address Data Management

The creation of a single accurate, managed data set, modelling both business and residential addresses, is an essential resource for any business improvement regime and a key component supporting the Council’s pledge for the customer to ‘tell us once’.

The Local Land and Property Gazetteer (LLPG) is a nationally recognised data set. This data set, when amalgamated with other local authority data sets provides the backbone of address location data for the whole of the UK. Every property across the UK is provided with a unique property reference number or UPRN. The Council will maintain an up-to-date gazetteer and where possible “seed” the UPRN across all Address based data sets to create a “golden address record” that will improve the consistency of address-based transactions.

7. Information Governance

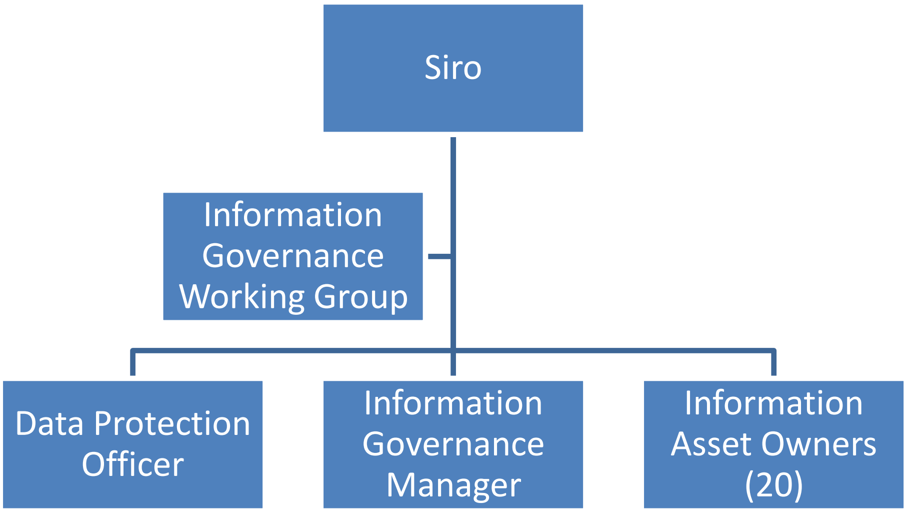
Information Governance is the effective use and management of the Council’s information assets which will enable us to obtain maximum value while minimising information-related risk. It encompasses all of the rules, regulations, legislation, best practice, standards, and policies that we need to comply with when we create, share, and use information.

The Council will adopt all necessary protocols and procedures to ensure the effective information governance of all data assets (paper & electronic) and other associated systems within the Council, as well as information held outside the Council that affects our regulatory and legal obligations.

Information Governance requires clear, effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. This requirement is set out in our Information Governance Framework. The Framework establishes roles and responsibilities and outlines how Information Governance policies and procedures integrate with other council policies, such as, Information Security, Records Management, ICT Acceptable Use Policy, Hybrid Working Policy (especially relevant now with the new **"ways of working"),** Internet and Email Policy, Retention and Disposal Schedules,

Information Governance Structure

The primary body responsible for the implementation of this policy is the Information Governance Working Group (IGWG). This group is chaired by the Council's Senior Information Risk Officer (SIRO). The SIRO is supported by the Data Protection Officer and the Information and Compliance Manager. In addition, Business Service based Information Asset Owners provide a link to service specific business areas.


Siro
Information Governance Working Group
Data Protection Officer
Information Governance Manager
Information Asset Owners (20)

The Data Protection Act and UK GDPR

The Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR) serves the purpose of protecting the privacy rights of living individuals. The DP Act 2018 and the UK GDPR requires the secure and lawful collection, processing, sharing and disposal of personal information whether on paper (including handwritten notes), in electronic form, video recordings on phones, computer/laptops or on other materials, such as CCTV images, images captured using Drones and voice recordings. The Council will ensure there is appropriate security cover when processing personal data in line with relevant guidance, rules, and regulations. The Council will respond to all requests for personal data submitted in line with the rights of individuals (Subject Access Requests)

Freedom of Information (FOI), Environmental Information Regulations (EIR)

The Council is required to actively publish information under the above Acts (including the Transparency Code 2015) as well as provide accurate, appropriate and timely responses to all requests received.

Data Privacy and Cyber Security

The risk of theft, damage to, or misuse of hardware, software and the information on IT systems is growing year on year as criminals become more creative in ways to steal or cause harm. This risk will only grow as more business processes are hosted on a variety of platforms including smart mobile devices, and a range of different networks. The Council continually reviews its vulnerability to cyber-attack as part of its cyber security strategy, identifying actions that are then implemented as part of the ICT Strategy.

Auditing and Review

The core aim of auditing and reviewing Information Governance process is to drive continuous improvement across the organisation. Therefore, this would require regular monitoring in order to keep up with the changing environment.

Information Governance 10 Key Statements

The Council's stance on information governance:

i. **Executive sponsorship**
No IG effort will survive and be successful if it does not have an accountable, responsible executive sponsor.

ii. **Stakeholder consultation**
Those who work most closely to information are the ones who best know why it is needed and how to manage it, so business units must be consulted in IG policy development. A cross-functional collaboration is needed for IG policies to hit the mark and be effective.

iii. **Information policy development and communication**
Clear policies must be established for the access and use of information, and those policies must be communicated regularly and succinctly to employees.

iv. **Information integrity**
We must ensure consistency in the methods we use when creating, retaining, preserving, distributing, and tracking information. We must adhere to good IG practices including data governance techniques and technologies to ensure quality data.

v. **Information organisation and classification**
We must establish standard formats, categorise all information, and semantically link it to related information.

vi. **Information security and privacy**
We must ensure we secure information in its three states: at rest, in motion, and in use at all times.

vii. **Information accessibility**
Accessibility is vital not only in the short term but also over time using long-term digital preservation (LTDP) techniques when appropriate (generally if information is needed for over five years).

viii. **Information control**
Appropriate document management data management, and report management software must be deployed to control the access to, creation, updating, and printing of data, documents and reports.

ix. **Information governance monitoring and auditing**
Information access and use must be monitored to ensure that guidelines and policies are being followed and to measure employee compliance levels.

x. **Continuous improvement**
IG programmes are not one-time projects but rather ongoing

Information Sharing and Stakeholders (Partners and Contractors)

The Council is well equipped to share and utilise data with relevant partners, ultimately adding to the delivery of effective and efficient public services coordinated around identified need. When seeking to share personal information, the council will continue to follow the good practice contained within the Information Commissioner's Data Sharing Code of Practice. The Council's Information Sharing Protocol must be followed when sharing information internally and with external stakeholders. The Council has signed up, and will continue with its commitment, to the Whole Essex Information Sharing Framework (WEISF).

The Council will always ensure it follows due process when engaging Contractors including working closely with the Procurement team. To ensure it meets all GDPR requirements, the Council has robust arrangements regarding data processing. Further information on internal and external stakeholders' structure with clear roles and responsibilities can be found in Appendix 2.

The Equality Act 2010: Public Sector Equality Duty

This policy is applicable to and will be communicated to, all Basildon Council staff, contractors, stakeholders, suppliers and third parties who interact with information held by the Council and the information systems used to store and process data. Employees are responsible for ensuring that they understand their responsibilities as defined in this policy and the supporting framework. Line managers are responsible for ensuring that all Basildon Council staff and contractors understand their responsibilities as defined in this policy and that they continue to meet its requirements for the duration of their employment/engagement. Furthermore, it is the line manager's responsibility to take appropriate actions if individuals fail to comply with this policy and the guiding principles.

Further information can be found in the Roles and Responsibilities Guidance, which outlines the roles and responsibilities associated with governance and management of information held by the Council. This includes information about data owners, data controllers, data processors, data protection officers, line managers, the chief information officer, information governance manager and more.

8. Council Ambitions

The table below provides a visual display of how this Policy will impact on the delivery of the Council's corporate plan Ambitions.

Corporate Ambitions 2021- 2024		**Levels of Impact**			
		High	Medium	Low	None
People	Healthy and active local communities supporting themselves and each other.		**X**		
Place	Safer neighbourhoods and towns		**X**		
Prosperity	Increased opportunity for all		**X**		
Good Governance: Fit for Purpose	Doing the right things, in the right way.	**X**			

9. Outcomes and Priorities

This policy seeks to achieve the following Outcome and Priorities:

Outcomes:

1. Full compliance with current legislation and updated best practice guidelines in relation to information management at Basildon Council
2. Establishment of a clear information management framework for future mapping of supporting policies, procedures and guidance
3. Public confidence in the Council's approach towards information management and data sharing.
4. Embedding of the principle that information is an asset, and therefore

understood, recorded, valued, protected, utilised and disposed of suitably.

5. On the Information Governance Maturity Model (IGM Model) (see Appendix 3), we considered that our current status is at the beginning of level 3 with the aim to be at level 4 by the next review date.

Priorities:

- Reduction in legal challenges posed to the Council based on a failure to adhere to data sharing and information management legislation.
- A triangulation of the Council’s digital transformation strategy, IT strategy and Information Management Policy Framework, ensuring mutual compatibility and collaborative working, enabling strategic alignment within the Council.
- Developing awareness about the associated statutory and regulatory requirements and responsibilities for information management
- Improved decision-making, policy formation, and general governance through the provision and utilisation of shared information.
- In relation to the IGM model, this is further explained in Appendix 3, we would be working towards level 4 by the next review date.

10. Links to other Corporate Policies or Partner documents

- ICT Security & Acceptable Use Policy ***(under review)***
- ICT Strategy
- Digital Inclusion Policy and Strategy (***in development***)
- Corporate Plan 2021-24
- Privacy Policy
- Information Management Framework (***under review***)
- Information Sharing Protocol (WEISF)

11. Glossary of Terms

- **Controller** – A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Data** – Is any collection of facts, images and sounds that are without context of meaning
- **Data Protection Officer** – Under the GDPR, some organisations need to appoint a data protection officer ('a suitably qualified dedicated resource available to deal with Data Protection compliance and obligations') who is responsible for informing them of and advising them about their data protection obligations and monitoring their compliance with them.
- **Data subject** – The identified or identifiable living individual to whom personal data relates.
- **Framework** – The structure of supporting policies, procedures, strategies and guidelines that will underpin information management. These will be refreshed and updated when necessary.
- **Information** – Is data with meaning. For example, 251221 is data, but it becomes information when we give the data meaning - Christmas 2021.
- **Personal Information** – Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- **Processing** – In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).
- **Processor** – A person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Records Management** – the administration of records and documented information for the entirety of its lifecycle.

12. Appendices

Appendix 1 – Applicable Regulation/Policy/Document Reference Table

Data Protection Act 2018, UK GDPR Privacy and Electronic Communications Regulation 2003
Freedom of Information Act 2000
Local Government Transparency Code 2015
Environmental Information Regulations 2004
Acceptable Use Policy
Public Records Act
Civil Service Code
The Government's 'Information Principles for the UK Public Sector'
The Information Sharing Principles from the Whole Essex Information Sharing Framework
Re-use of Public Sector Information 2005
Transparency Code 2015
ICO Data Sharing Code of Practice

Appendix 2 - Stakeholders' Roles and Responsibilities

This section sets out the specific roles and responsibilities in relation to good Information Governance within the council

Directors and managers are responsible for ensuring:

- All staff are aware of and comply with this policy
- All staff are aware of and comply with relevant data handling procedures within their service area
- All staff have undertaken training as necessary

The Senior Information Risk Owner (SIRO) will:

- Take overall ownership of Information Security
- Act as champion for Information Risk at Strategic Leadership Team (SLT)
- Implement and lead on the Information Governance risk assessment and management processes within the council and advise SLT on the effectiveness of information risk management;
- Chair the Council's Information Governance Working Group
- Works in conjuction with the DPO in regards to reportable data breaches.

Head of ICT Resilience and Information Governance will:

- Ensure Information Security and Business Continuity arrangements are appropriate
- Works in conjuction with the SIRO and the DPO in regards to

reportable data breaches.

- Act as the access route to SLT on behalf the Information Governance Group.

Information Asset Owners (IAOs) The role of the IAOs is to:

- Understand what information is held within their teams, how it is use; where it is stored; whether it is shared, either internally or externally; who has access to it and why and how long it is retained for, in order for business to betransacted within an acceptable level of risk.
- Understand and address risks to the information assets they ‘own’ and provide assurance to the SIRO on the security and use of these assets.

The Data Protection Officer (DPO) is responsible for ensuring compliance with relevant legislation. In addition, the officer will:

- Monitor internal compliance with data protection legislation. This is primarily the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Freedom of Information Act 2000 (FOI), Environmental Information Regulations 2004 (EIR)
- Ensure suitable data protection policies are in place
- Inform and advice on data protection obligations, including the provision of relevant training;
- Provide advice regarding Data Protection Impact Assessments (DPIAs)
- Sign off DPIAs/DPAs and ISAs
- Act as a point of contact for data subjects and the information Commissioner’s Office (ICO).

The Information and Compliance Manager is also responsible for ensuring compliance with relevant legislation. The officer will:

- Monitor internal compliance with data protection and access to information legislation. This is mainly the UK General Data Protection Regulations (UK GDPR) and Data Protection act 2018.
- Ensure suitable Information Management policies are in place
- Inform and advise on information management obligations, including the provision of relevant training;
- Provide advice regarding Data Protection Impact Assessments (DPIAs)
- Provide advice and guidance on Data Processing Agreement (DPAs) or Information Sharing Agreements (ISAs)

Elected Members and Staff (including temporary and interim) are responsible for:

- Complying with this and other relevant policies and procedures covering the use and security of all information and, in particular, personal, sensitive or confidential information.

All contractors, consultants, partners or other agents of the council must:

- Understand the value and sensitivity of Council’s information and treat it accordingly
- Ensure that they and their staff who have access to personal information held or processed for or on behalf of the council are aware

of this policy and are fully trained in and aware of their duties and responsibilities under the UK GDPR and Data Protection Act 2018. A breach of any provision of data protection legislation will be deemed as being a breach of any contract between the council and that individual, company, partner or firm.

- Comply with the Council’s data protection process by contributing to the completion of a DPIA and adhere to DPA and ISA protocols where appropriate.
- Allow checks to be carried out by the council as part of its (due diligence process) of personal information held and processed on its behalf to ensure such processing is in complaince with any agreements in place.
- Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, indemnity as per contract agreement.

Suitable third party processing agreements must be in place before any processing of personal data for which the council is responsible is undertaken by any third party.

Appendix 3 - Information Governance Maturity Model

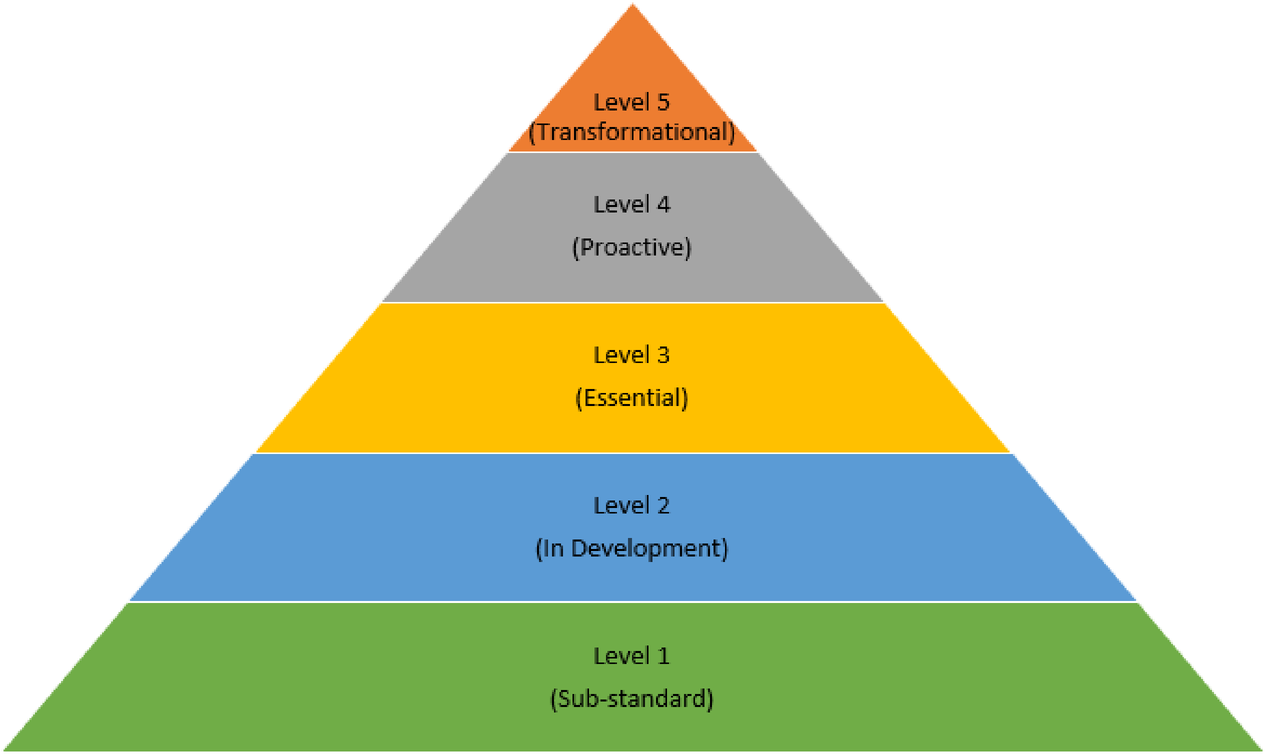
- **Level 1 (Sub-standard):** This level describes an environment where recordkeeping concerns are either not addressed at all or are addressed in a very ad hoc manner. Organisations that identify primarily with these descriptions should be concerned that their programmes will not meet legal or regulatory scrutiny.

- **Level 2 (In Development):** This level describes an environment where there is a developing recognition that recordkeeping affects the organisation, and that the organisation may benefit from a more defined information governance programme. However, in Level 2, the organisation is still vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely ad hoc in nature.

- **Level 3 (Essential):** This level describes the essential or minimum requirements that must be addressed in order to meet the organisation's legal and regulatory requirements. Level 3 is characterised by defined policies and procedures, and more specific decisions taken to improve record keeping. However, organisations that identify primarily with Level 3 descriptions may still be missing significant opportunities for streamlining business and controlling costs.

- **Level 4 (Proactive):** This level describes an organisation that is initiating information governance programme improvements throughout its business operations. Information governance issues and considerations are integrated into business decisions on a routine basis, and the organisation easily meets its legal and regulatory requirements. Organisations that identify primarily with these descriptions should begin to consider the business benefits of information availability in transforming their organisations globally.

- **Level 5 (Transformational):** This level describes an organisation that has integrated information governance into its overall corporate infrastructure and business processes to such an extent that compliance with the programme requirements is routine. These organisations have recognized that effective information governance plays a critical role in cost containment, competitive advantage, and client service.



Monday to Friday
10am to 5pm

BasildonCouncil
BASILDON • BILLEIU(AY • WICKFORD

For translations, Large Print and Braille please call

Para olbtener traducciones, por favor llame al numero (Spanish)

'61-fllllt \lliMfi:rnT (Bengali)

Aby l!Jzyskac pisemne tll!Jmaczenie prosz dzwonic pod nl!Jmer (Polish)

:tz□ ft w, *iffr&tT* (Mandarin)

O preklad prosim zavolejte (Czech)

IJI , ffi3&'il (Cantonese)

4T06bl nony4t.1Tb nepeBO;Q Ha PYCCKl'1H 3blK, no3BOHl'1Te no renecpoHy (Russian)

TercGme i9in lutfen araym (Turkish)

oj,.,.,!;.6.!I L;i½*Ji* **iJI** (Farsi)

Pour obtenir une traduction, composez le (French)

!So_,Lo;*9-!* o u,990Jo:; 0..09-;o:.; .9-!(Kurdish)

'')'I *(FI-* 4JUJ (Arabic)

Per perkthim me shkrim ju lutem memi ne telefon (Albanian)

oo"cti11. iu.2 ,11 h:fl tit"1. !:it (Gujarati)

<1i cfit: (Hindi)

Pentru traducere va rugam sunati (Romanian)

Untuk terj:emaha11 harap hubungi (Indonesian)

Kwa tafsiri, tafadhali piga simu (Kiswahili)

c{'E cfa"(Punjabi)

Kana muchida kuturikirwa, tapota ridzai runhare kuna (Shona)

Pre preklad prosim volajte (Slovak)

Neu qui vj can djch tai lieu, xin vui long gQi theo SO (Vietnamese)

01268207955

Language Line services

Customers with a hearing or speech impairment can contact us using the Text Relay service. Dial 18001 followed by the full telephone number of the service you require. Calls are charged at your telecommunications provider's standard rate.

This page is intentionally left blank