Records Management Policy

Document Control

Organisation	Barnsley Metropolitan Borough Council
Title	Records Management Policy
Author	Licensing and Records Specialist
Filename	Records Management Policy
Owner	Governance and Compliance Manager
Subject	Records Management
Protective Marking	Official
Commencement Date	25th May 2018
Applicable to	Council Members, employees, contractors/agents working for or on behalf of the Council and partner organisations
Information/ Action	For information and appropriate action to comply with the policy
Review Date	1 year from date of approval or when changes in law or best practice guidance
Review Responsibility	Information Governance Board

Revision History

Date	Version	Author	Comments
April 2018	0.1	ICT Manager / Information and Records Manager	Revised policy and amendments following consultation
May 2018	1.0	ICT Manager / Information and Records Manager	Approved
September 2018	2.0	ICT Manager / Information and Records Manager	Minor amendments to staff titles due to organisational changes
December 2019	3.0	ICT Manager/Information and Records Manager	Amendments to email retention and desktop use
April 2020	4.0	Information and Records Manager	Addition of section 6.1.6
August 2021	5.0	Licensing and Records Specialist	Amendments to staff titles and UK GDPR, addition to section 6.1.6
February 2023	5.1	Information Governance and Security Incident Analyst	Amendment to document owner
12/05/2023	5.2	Head of Design & Compliance	Reviewed
May 2023	5.3	Information Governance Board	Issued for review/approval
May 2023	6.0	Published	

Document Distribution

This document will be distributed to the following for review and feedback prior to submission for approval:

Name
Information Governance Board
Senior Management Team
Trade Unions

Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – The person(s) responsible for developing and introducing the policy
- **Accountable** – The person who has ultimate accountability and authority for the policy
- **Consulted** – The person(s) or groups to be consulted prior to final policy implementation or amendment
- **Informed** – The person(s) or groups to be informed after procedure implementation or amendment.

Responsible	Information Governance Board
Accountable	Governance and Compliance Manager
Consulted	BMBC Information Governance Board, Senior Management Team, Trade Unions
Informed	Council Members, employees, contractors/agents working for or on behalf of the Council and partner organisations

Table of Contents

1 Introduction

The Council recognises that their records are an important means of providing evidence of activities, actions, decisions, and transactions that support the business and operating decisions of the organisation.

Records Management is a corporate function that is responsible for the systematic and comprehensive control of all records from their creation or receipt, through their processing, distribution, organisation, storage, and retrieval, to their ultimate disposition.

The establishment of an effective and efficient record keeping environment ensures standardisation, protection, and retrieval of information, thereby improving levels of quality customer service and ensuring effective information management and retrieval throughout the Council.

The Council must comply with all relevant legislation, national standards, and codes of best practice, including, but not limited to:

- The Data Protection Act 2018
- UK General Data Protection Regulations 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Limitation Act 1980
- Local Government Act 2000
- ISO 15489 (International Standard for Records Management)
- Lord Chancellor's Code of Practice (Section 46 of the FOIA 2000)

In addition services will have specific legislation for their own service area, for example:

- Foster Care Supervision and Support – The Fostering Services Regulations 2002
- Adoptions Management – The Disclosure of Adoption Information Regulations 2005

This policy defines the Councils responsibilities and activities in regard to both paper and electronic records and provides the framework for specific business unit and service guidance and detailed operating procedures.

The purpose of this policy is to establish a framework for the implementation and development of a Records Management programme that will ensure the Councils records meet the requirements of relevant legislation, codes of best practice and national standards in an economical, efficient, and effective manner.

The policy concerns the life cycle of the records which are created, used, maintained, and disposed of in the conduct of the Council's business activities

A record is defined within the ISO 15489 as 'any form of information created and maintained that documents a business transaction or decision or that is required to meet legal or financial obligations regardless of format or medium'.

2 Aim

In summary, this Policy aims to ensure that a suitable infrastructure, based upon national standards and codes of best practice, is in place in order to ensure that the Council:

- Creates and captures accurate, complete, authentic, and reliable records which demonstrate evidence, accountability and information for its decisions, actions, transactions, and activities;
- Efficiently and effectively maintains the integrity of records to meet the Council's operational and administrative requirements;
- Identifies records that are linked to critical activities and ensures they are accessible to allow continuity of service during any disruptions;
- Disposes of records that are no longer required in an appropriate and secure manner in accordance with the agreed Corporate Retention Schedules;
- Prevents the premature disposal of records;
- Protects the interests of data subjects and complies with the requirements of Data Protection Laws;
- Protects the legal rights of the Council, its clients and others affected by its actions;
- Provides appropriate and effective security to protect vital records from accidental or unauthorised access, loss, alteration, corruption, destruction, misuse, or leakage;
- Ensures records remain accessible to authorised users;
- Facilitates audit and examination of the Council's business;
- Maintains a Publication Scheme that provides permitted information to members of the public and others;
- Provides access to permitted information as defined within the Freedom of Information Act 2000;
- Makes appropriate arrangements for the recovery of records and operations in the event of an unplanned event occurring;
- Complies with all the prevailing legislation, regulations, and Government directives;
- Preserves records of historical permanent interest;
- Makes all employees aware of the importance of Information Management and of their areas of responsibility through appropriate training, including upon induction; and
- Ensures records are not kept in contravention of legislation or for longer than required.

The Council aims to develop a council wide approach to filing classification and move towards an Electronic Documents and Records Management System (EDRMS). SharePoint is the Council's primary record management system utilised to encourage the change from mainly paper based systems to electronic records management.

Scope

This Policy applies to all Council Members, employees, contractors/agents working for or on behalf of the Council and partner organisations. All Council employees have a responsibility to effectively manage their records and comply with the prevailing legislation and standards. All employees should recognise that all the records they create, receive, or maintain in the course of Council business are the official records of the organisation.

For the purposes of this Policy, a record is defined as being any information held by the Council irrespective of the medium, including the following:

- Handwritten documents

- Printouts
- Electronic records
- Electronic Document and Record Management Systems (i.e. SharePoint)
- Business and Information Systems (i.e. TED, SRM7, SAP)
- Microfilm or Microfiche
- Maps
- Drawings and Plans
- Photographs
- E-mails
- Teams chat messages
- Website content
- CCTV footage
- Audio-visual media

The Policy applies to all the records of the Council, during their lifecycle, from creation through to final disposition including disposal or where required, permanent preservation.

3 Policy Principles and Purpose

Accountability – records should be maintained to account fully and transparently for all actions taken and decisions made. They should provide credible, reliable, and authoritative evidence to facilitate an audit and protect the legal and other rights of employees or others affected by those actions.

Accessibility – records and the information within them can be efficiently and accurately retrieved by those with authorised access to them, to aid decision-making and increase management effectiveness, and meet the responsibilities of being open, honest, and transparent to the public.

Quality – records will be complete, accurate and reliable so that their authenticity can be guaranteed. Records will only be retained for the recommended time specified within the Corporate Retention Schedule in order to comply with the Freedom of Information Act and Data Protection Laws.

Security – records will be held in an appropriate format that will ensure they will be readable for as long as they are required. Records will also be secure from unauthorised or inadvertent alteration or erasure and all access and disclosure will be properly controlled. Audit trails will track all use and changes.
Retention and disposal – there will be consistent and documented retention and disposal procedures to include the provision for permanent preservation of archival records.

Training – all employees should be made aware of their record management responsibilities and guidance can be provided by the Council's Licensing and Records Specialist and Information Governance team to enable them to carry out their work efficiently and effectively.

Performance measurement – the application of records management procedures will be regularly monitored against agreed indicators and action taken to improve standards, as necessary.

Procedures – all records management procedures will be documented and made available on the Council's intranet pages.

Preservation – the corporate memory of the Council will be preserved (the loss of information when employees depart will be curtailed) and vital records will be identified and stored appropriately including the corporate electronic memory.

Audit - All records will meet audit requirements, be managed in accordance with procedures under Data Protection, the Freedom of Information Act, the Environmental Information Regulations Act, Copyright Legislation, and the Human Rights Act.

Purpose

The implementation of the Records Management Policy will be managed by the Governance and Compliance Manager and will include the following milestones/deliverables:

- Establish current record keeping practices and requirements;
- Oversee a classification scheme to ensure records that demonstrate Council decisions and actions are created and/or captured;
- Maintain retention schedules specifically for the Council which gives explicit reasons for retention periods and make readily available to all employees;
- Maintain a disaster recovery and business continuity plan to protect the Council's vital records;
- Manage procedures for the creation, maintenance, and disposal of all the Council's records;
- Establish the design and implementation of new record keeping systems which incorporate records management requirements;
- Maintain all current record keeping systems which incorporate records management requirements;
- Promote storage of records at the Councils contracted offsite storage location;
- Assist with the implementation of Records Management software solutions such as ECMS, based on an assessment of needs and existing practices and systems;
- Monitor compliance with the policy through the use of Key Performance Indicators and annual reviews;

This policy will take immediate effect and supersedes all previous Records Management policies.

If anyone has any queries in relation to the policy, they should initially discuss them with their line manager. Further advice and guidance can be obtained from the **Records Management** intranet site.

4 Roles and Responsibilities

Senior Management Team - Ownership of the Records Management Policy including approving the framework for managing and overseeing Council duties in relation to records management as set out in this policy.

Licensing and Records Specialist - Will develop and implement the records management policy, standards, and best practice guidance. Also monitor and report on the compliance of the Records Management Policy. Provide a strategic focus for record keeping throughout the Council and ensure that records management procedures are implemented and adhered to by service users.

Service Directors - Implement the policy within their business units ensuring their staff will liaise with the Licensing and Records Specialist on the management of records within the services for which they are responsible.

Employees and Elected Members - All Council staff have a duty to ensure the accuracy, integrity, and security of records that they access and use in the course of their work. They will create records to support the conduct of their business activities, registering records into paper or electronic record keeping systems. They will learn to differentiate between documents and records and learn how and where records are kept within the Council and will not destroy records without reference to the Corporate Records Retention Schedule or authority from the Licensing and Records Specialist. They will not lose records and will be aware of and adhere to the records management procedures. They will ensure that records in relation to their work are authentic and reliable and understand the limit of their authority to create, view, disclose or delete records. Employees with specific responsibilities for records management over and above those described here will need to have these clearly defined in their job descriptions. All records created by Council employees and Elected Members will remain the property of the Council.

The Customer, Information and Digital Service are responsible, as appropriate, for the design, building, maintenance, operation of systems in which electronic records are generated and used, and for the technical operation of computer and communication systems.

5 Best Practice and Related Guidance

Records will be managed in accordance with relevant codes of practice for records management and all relative regulation and legislation. This policy should be read in conjunction with other relevant policy and procedural documents highlighted within this policy.

6.1.1 Records Management Recovery and Business Continuity (Disaster Planning)

The implementation of the Records Management Policy includes maintaining a disaster recovery and business continuity plan to protect the Council's vital records.

- A risk assessment of potential disaster events identifying threats to records and recordkeeping systems will be performed and documented within the 'Disaster Recovery and Business Continuity Plan' in each Directorate/service area.
- Preventative measures for protecting vital records are documented and implemented within the Disaster Recovery and Business Continuity Plan for each Directorate/service area.
- Vital records will be identified and documented in an information asset register.
- Vital records protection including recovery and restoration procedures will be incorporated in the 'Disaster Recovery & Business Continuity Plan' for each Directorate/service area.
- Protective measures will be in place at the Councils contracted offsite storage facility such as:
  - Smoke and heat detectors
  - Fire extinguishers
  - Security fittings on doors and windows e.g. metal shutters, locks, and keypads
  - CCTV
  - Burglar Alarms

The Disaster Recovery and Business Continuity plan for all Council buildings can be found on the Health and Safety – Emergency Resilience intranet site.

6.1.2 Record Keeping / Creation of Records

The Council will ensure that records are kept for business, regulatory, legal and accountability purposes. Each operational or functional unit of the Council should have in place an adequate system for documenting its activities. This system should consider the legislative and regulatory environments in which the organisation works.

Records of a business activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities.

Records created by the Council should be arranged in a record keeping system that will enable the
Council to obtain the maximum benefit from the quick and easy retrieval of information. Official Council records should not be stored on Desktops, OneDrive's or Outlook but instead should be saved in a central location with the appropriate permission controls applied.

Records systems will be designed to enable or provide:

- Quick and easy retrieval of information;
- Routine records management processes to take place;
- The context of a record and its relationship to other records to be understood;
- The audit trailing to be maintained;
- Business continuity;
- Secure storage;
- Protection from accidental or unauthorized alteration, copying, movement or destruction;
- Protection from unauthorised access and misuse.

Individual Council employees are responsible for ensuring that both records and documents are stored in the correct location and not in breach of any confidentiality or copyright laws. This

includes the use of OneDrive for Business which provides all Council employees with a secure personal document storage space for personal documents such as training materials and certificates, one-tone notes and other ephemeral documents.

Council employees must ensure that no business records, copyright pictures and copyright music or videos are stored on OneDrive's or Desktops. Any and all records created for work purposes belong to the Council and should be stored in a central shared location. All documents stored on OneDrive's will be deleted as part of the starters, movers, and leavers policy. In addition, from 1st February 2020 all emails will be automatically deleted from outlook after 12 months (from date received) meaning all records held in this format must be transferred to the appropriate system (SharePoint) as soon as possible.

The Council has an inventory of all of its **information assets** which helps to promote control over records and provide valuable data for developing record appraisal and disposal procedures.

The creation of duplicate records and the proliferation of various versions will be strongly avoided. In addition ephemeral records (non-records) should be routinely destroyed.

Paper and electronic record keeping systems should contain metadata (descriptive and technical information) to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records

The record keeping system, whether paper or electronic, should include a set of rules for referencing, titling, indexing and, if appropriate, the security marking of records. The Council will introduce an Information Classification Handling Policy as the basis for identifying how information and records can be disclosed and determining the required level of security measures to be applied.

Effective access controls should be used to ensure that only authorised users can gain access to the functionality of the relevant records systems. Such access should be tailored to the user's role and position so that only the required functions can be accessed.

Service areas will ensure that Council staff are suitably trained in the creation and use of records and also provide supporting documentation for each record keeping system.

Procedures should be in place to ensure the currency, accuracy, and completeness of Council records.

6.1.3 Record Maintenance

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.
Records should be stored in an environment that provides the required levels of security and protection to prevent unauthorised access, damage, or loss, whilst allowing maximum accessibility to the information related to its frequency of use.

Electronic records, files, databases, and application systems will be subject to suitable periodic backup routines. In practice these may be undertaken by either, IT or a nominated System Administrator. In order to ensure the viability of back-up records for business continuity and

recovery purposes, they should be subject to periodic verification during recovery and Business continuity testing.

Records no longer required for the conduct of current business should be identified and, if appropriate, transferred to a secure place of storage. Due account must be taken of the requirements of the Corporate Retention and Disposal Guidelines with respect to the periods for which the Council is obliged to retain specific records.

6.1.4 Record Disposal

Record disposal, in this Policy, relates to the point in the record lifecycle where records are either transferred to the Council's contracted offsite paper storage facility, archived (Town Hall Archive) or destroyed.

While it is essential to retain data which is required to manage the business, it is equally important to dispose or archive data which is no longer required and past its specified retention period.

The retention and disposal of records when they cease to be in active use will be primarily determined by the prevailing legislative and regulatory requirements and business needs.

Record Retention and Disposal Schedules determine, *inter alia*, the legislative or regulatory requirements for record retention. There are also arrangements in place for records disposal for **Academy Schools**.

Each Directorate must have in place clearly defined arrangements for the appraisal and selection of records for disposal.

Records should be closed as soon as they have ceased to be of active use other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed should be shown on the record itself as well as noted in the index or database of the files/folders. Wherever possible, information on the intended disposal of electronic records should be included in the metadata when the record is created. The storage of closed records awaiting disposal should follow accepted standards relating to environment, security, and physical organisation.

Directorates will have in place systems for managing the appraisal of records and indicating what records are designated for destruction. The system will also record the authority under which the records are to be destroyed, when and how they will be destroyed, any legislative provisions, functional context, and physical arrangements. This information will provide valuable data for placing records selected for preservation into context and will enable future records managers to provide evidence of the operation of the Council's Corporate Retention and Disposal Guidelines. Records will be reviewed at the end of their prescribed retention period considering the value and purpose of their continuing retention. Any decision to retain records beyond their prescribed retention period will be documented and agreed by the relevant Director in consultation with the License and Records Specialist. Records selected for permanent preservation and that are no longer required for operational use by the Council, will be transferred to the Council's place of deposit, the Council's secure archive (Town Hall) and these will be transferred in accordance with the legislation and regulations prevailing at the time of review.

Records that have not been selected for permanent preservation and which have reached the end of their administrative life will be destroyed in a secure manner as is necessary for the level of confidentiality or protective markings they bear. In relation to records containing personal or sensitive information (as defined by Data Protection Laws), their destruction will fully support the principles contained within these laws.

Paper records held at the Council's contracted offsite storage facility which are due for disposal in line with the retention period will be disposed of via the Council's confidential waste arrangements through the services of suitably certified contractors. Any contractors used for onsite shredding must be monitored at all times and must provide a disposal certificate upon completion. All disposal logs and certificates must be retained indefinitely by the service to which the records belong in order to maintain the appropriate audit trail.

Disposal of confidential records or records containing personal data other than those stored at the Council's contracted offsite storage facility should be shredded at source immediately after administrative use is concluded. Confidential records or records containing personal data should not be disposed of in the paper recycling bins.

All IT hardware will be disposed of via approved contractors via IT service desk. Directorates/service areas will not dispose of or sell IT hardware or equipment.

If a record due for destruction is known to be the subject of litigation or a request for information, destruction should be delayed until disclosure has taken place or, if the Council has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act 2000 have been exhausted and the legal hold lifted.

6.1.5 Electronic Records

The principal issues for the management of electronic records are the same as those for the management of any record. They include the creation of authentic records, the tracking of records and disposal arrangements. However, the means by which these issues are addressed in the electronic environment will be different.

The Council will apply and promote the following requirements in relation to electronic records:

- A clear understanding of the nature of electronic records used throughout the Council, with their details being contained within the Information Asset Register;
- The creation of records and metadata necessary to document business processes as part of the system that holds the records;
- The maintenance of a structure of folders (see corporate file plan) to reflect the logical groupings of records;
- The secure maintenance of the integrity of electronic records;
- The accessibility and use of electronic records for as long as required, which may include their migration across systems or applying some form of digital preservation in the event of the current media or system becoming unsustainable;
- The application of appropriate disposal procedures including procedures for archiving;
- The ability to cross reference electronic records to their paper counterparts in a mixed environment;
- An audit trail will be maintained of transactions and systematic actions relating to records. The audit trail and other system logs will be securely retained relative to their criticality

and be made available, as required, for inspection by Internal Audit or other authorised persons.

6.1.6 Electronic Communication and Collaboration Platforms

Council employees are expected to utilise all electronic communication and collaboration tools, such as Microsoft Teams, in line with all existing Records Management, Information Security and Information Governance Policies and guidelines. Communication tools such as email, Microsoft Teams Recordings and Microsoft Teams chat messages are legally enforceable and legally disclosable and thus are subject to the Public Records Act, Freedom of Information Act 2000, and Data Protection Laws. All Council employees are expected to use such tools in a business appropriate manner and where necessary manage these in line with the principles stated within this policy. All business actions and decisions, which may be required as evidence, must be documented in an official record (not just via Teams or Email) and stored in a central location with the appropriate permissions and retention periods applied.

Employees are prohibited from recording meetings, unless absolutely necessary, due to concerns regarding legal disclosure (Freedom of Information and Subject Access requests). The unnecessary use of these formats could leave the Council, its staff, and its service users vulnerable to Data Protection and legislation breaches.

Exception: Internal Audit / Fraud team may undertake an interview under caution and use a PACE compliant recorder.

For further guidance regarding the use of Email and Microsoft Teams please see the Records Management Quick Reference Guides available here.

6.1.7 Access

The Council's employees are only granted access to information that is related to their duties. A system of access control is in place which controls access to electronic information systems and records. Any actual or attempted breaches of access control are regarded as a disciplinary offence.
Physical security measures are in place to provide protection of Council records from unauthorised access, loss, damage, or destruction.

Documents not included within the Council's Publication Scheme may be available, upon request, under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, or the Data Protection Laws. The Council has established separate policies and documented staff guidance for the Freedom of Information Act, the Environmental Information Regulations and Data protection so as to ensure compliance with the legislation when dealing with requests and defines certain categories of exemption.

6.1.8 Training and Awareness

Managers will ensure that all staff with responsibility for managing records are appropriately advised, trained and aware of the requirements of best practice for records management.

6.1.9 Performance Measurement

The application of sound systems of Information and Records Management across the Council will be subject to ongoing review involving, where appropriate, System Owners, Information Asset Owners, System Administrators, Internal Audit, IT Managers, and the IT Security Lead.

The timing of responses to requests for information records under the Freedom of Information Act and Data Protection Laws is recorded as a means of ensuring that they fall within the prescribed response timescales.

The annual performance of the adopted Information Governance framework will be agreed by the Information Governance Board.

6.1.10 Compliance with the Records Management Policy

All breaches of the Records Management Policy will be treated with utmost concern and, in respect of employees, investigated as an allegation of potential misconduct/gross misconduct in accordance with the Council's Disciplinary Procedure. Further guidance can be found on the HR intranet page (Disciplinary Procedure).

6.1.11 Further Guidance

The Council has established and implemented a range of other Policies and Procedures in support of Records Management and these can be located on the **Information Governance** and Records Management intranet sites.
Enquires on matters related to Data Protection, IT Security and any other information governance issues should be directed to the **Information Governance** intranet site.

6.1.12 Policy Review

This policy will be reviewed every 12 months and updated in the interim as required.

The periodic reviews will be conducted by the Governance and Compliance Manager and endorsed by the Information Governance Board.

Appendix 1 – Glossary of Terms

Term	Definition
Active (or Current) Records	Records that are required frequently and that need to be accessible by staff on an ongoing basis. (An active record can be subsequently closed in accordance with the Retention and Disposal Guidelines and either stored or disposed of as required).
Archival Records	These are records designated as having a long-term regulatory, historical, cultural, or educational significance and requiring appropriate archiving (either within the Council or with a recognised local or national body).
Compliance	In the context of Information and records management, compliance relates to the Council's need to operate in accordance with the existing legislation, regulations, and codes of best practice.
Data	Data can be thought of as the smallest component of information, but which does not necessarily have meaning, such as individual letters and digits held in a random way. For example, 0850361974 is a string of numbers. On their own, and out of context, it can be almost impossible to tell what the numbers refer to, but they are data (in this case, an ISBN number which identifies a book).
Data quality	Data quality relates to the accuracy, integrity, completeness and reliability of data and information.
Data Subjects	Data Subject relates to the individual who is the subject of the personal data. In practice, we are all Data Subjects. Data Protection Laws grant rights to Data Subjects to see the data stored about them and requires that any errors in the data be corrected. In some circumstances the Data Subject may have a right to compensation for damage or distress caused.
Disposition/Disposal	This is the final stage in the record lifecycle and can either relate to destruction or transfer to a recognised archive for preservation. The Retention and Disposal Guidelines will define any statutory or regulatory requirements for the internal retention of records (for example for VAT accounting purposes).

Term	Definition
Ephemeral (non-records) information	A document containing information of short term or transitory value; of use for the duration of a particular activity or a duplicate copy for consultation purposes. Ephemeral documents are not transferred to a records system but are immediately disposed of after use.
Information	Information is something which tells us something and can also be communicated to someone else in a meaningful way. Information is data that is put into context, can be comprehended, understood, and shared with other people and / or machines.
Information governance	Information Governance is an encompassing term that relates to all laws, regulations, policies, procedures and protocols for the creation, use, amendment, storage, release, sharing, re-use disposal and destruction of all information held by the Council.
Information management	A management framework for the acquisition, organisation, storage, security, retrieval, use, sharing, dissemination, and disposal of information.
Information resources	Information resources are the physical objects and digital code and files that store information. A book is a paper information resource. A pdf file is a digital information resource. The term 'information resource' is used throughout this policy document as a generic term. It can mean a record within a database, or the whole of the database. An information resource can also be an html page, or the whole of an Internet or intranet site.
Information security	The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity, and availability of information.
Information Steward	The officer responsible for the accuracy, integrity, and quality of data within their domain. Information Stewards are trustees of information rather than the owners of the information and the related systems.
Knowledge	Knowledge implies understanding. Knowledge could be defined as information plus experience and opinion.

Knowledge management	The Process responsible for gathering, analysing, storing, and sharing knowledge and information within an Organisation.

Term	Definition
Metadata	Metadata is data about data, giving details about the context, content, and structure of the record. Metadata supports retrieval, establishes provenance, and demonstrates links between documents and relationships between records, aids the integrity of records and the ongoing use of the record as technological platforms evolve over time. Metadata is also used in the classification of records as a means to identify the related security requirements.
Non-Active (or NonCurrent) Records.	These are records that are no longer referred to in the course of the Council's daily operations, but that must be retained in accordance with the Council's Retention and Disposal Guidelines.
Personal Data	Personal Data is information that relates to a living individual who can be identified from that information (or from that and other information in the possession of the Data Controller), including any expression of opinion about the individual and, with very few exceptions, any indication of the intentions of the Data Controller in respect of the individual.
Processing	Any activity/operation performed on data, whether held electronically or manually, such as obtaining, recording, holding, disseminating, or making available the data or carrying out any operation on the data. This includes, organising, adapting, amending, and processing the data, retrieval, consultation, disclosure, erasure, or destruction of the data.
Records	Information created, received, and maintained as evidence and information by the Council, in pursuance of legal obligations or in the transaction of business.
Records management	The discipline and professional function of managing records in order to meet organisational needs, business efficiency and legal and financial accountability.

Semi-Active (or SemiCurrent) Records.	These are records that are required to support the Council's operations, but which are only accessed on an infrequent basis.

Term	**Definition**
System Owner	Normally senior managers who have overall operational responsibility for the operation and security of the systems and information used within their service or functional areas.
Structured Data	Structured data is highly organised and formatted in a way that allows easy retrieval. For example, customer names, transaction info, dates, phone numbers etc.
Unstructured Data	Unstructured data has no pre-defined format or organisation, making it difficult to collect, process and analyse. For example, Word processing documents, emails, images, audio, and video files etc.