Records Management Policy

Policy summary

Purpose	This policy sets out Dorset Council's commitment to achieving high standards in records management in order to meet its strategic objectives, legislative and regulatory obligations, mitigate risk and adhere to best practice standards.
Scope	Dorset Council creates, receives and manages a wealth of information that is essential for delivering a diverse range of services and fulfilling legal obligations. This policy applies to information from all business activities and work locations. Records management is concerned with the capture and management of records and the information they contain. For the purposes of this policy, 'records management' is a broad collective term that refers to all recorded information (records, documents and data) regardless of format, storage location or media on which it is created. This scope includes, but is not limited to: • digital – Office documents, files held on network drives or in M365, data held in software applications, scanned records, emails, chats and posts in Teams, text messages such as WhatsApp, and social media such as Twitter • hard copy paper files, microfiche or microfilm • audio and video recordings, photographs, slides, and multimedia content • building maps and plans • websites and intranet sites that provide information to employees or members of the public • relevant metadata (data about the context, content and structure of other records listed above) This information belongs to Dorset Council and all individuals and teams entrusted with it must manage it appropriately in line with this policy.

Table of contents

Glossary

Archive - (1) To permanently retain records that are of value for corporate memory or historical purposes. (2) A place for keeping records permanently. (3) The body of documents and records formed by an organisation in their course of their work selected for permanent preservation. The Records Management Service works closely with Dorset History Centre to transfer a proportion of records to be preserved as corporate memory for future generations. Contact archives@dorsetcouncil.gov.uk for any enquiries regarding Dorset History Centre services or collections, and to offer material that relates to the history of Dorset.

Records - information created, received and maintained as evidence and as an information asset in the course of council business. Any set of information, regardless of its structure or form, can be managed as a record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business (source: ISO 15489-1 Records management concepts and principles)

Records management - discipline responsible for the efficient and systematic control of records through their lifecycle from creation to destruction or preservation as archives.

Records management system - system or procedures for capturing, managing and providing access to records over time.

Records lifecycle - the distinct phases of a record's existence, from creation to disposal.

Disposal - the decision about what happens to records once their minimum retention period has been reached. This moves records to the last stage of their lifecycle, which can either be complete destruction, transfer to an organisation that has taken responsibility for the function, or permanent preservation as archives.

Vital records - records without which the Council would be unable to function, or to prove that a key activity has taken place.

Senior Information Risk Owner (SIRO) - the role responsible for managing information risk at the highest level.

Information Asset Owner - designated senior managers responsible for monitoring the risks to information held in their service. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

Information Asset Register - a simple catalogue to understand and manage information assets and the risks to them. An information asset is any grouping of information, physical or digital, that has value in supporting your service's work.

1. Introduction

1.1 The Records Management Policy aims to ensure that Dorset Council proactively manages records throughout their lifecycle, regardless of format.

1.2 Records are both a valuable resource and an important asset. As with any asset, such as people or property, records require proper management. They support effective service delivery, provide evidence of our activities and decisions, and maintain the corporate memory.

1.3 The benefits of systematically managing our records are:

- Protecting our most important information and improving business resilience and efficiency
- Making sure information can be found and retrieved quickly and accurately
- Complying with legal and regulatory requirements, particularly the Freedom of Information Act, the Data Protection Act 2018, and the UK General Data Protection Regulation
- Mitigating information risk; avoiding fines and protecting our reputation
- Minimising storage requirements and reducing costs

1.4 Effective records management helps to ensure that the correct, accurate and up to date information is easily available to the right person, at the right time, when needed. This policy therefore underpins effective decision making, good governance, transparency and accountability in the management of services.

1.5 This policy defines the direction Dorset Council is taking in recognising records management as a core corporate function. Fully embedding this policy is under development, will be closely informed by service design and will be subject to iterative review over time. Currently, the Records Management service is part of Archives and Records within Customer Services, Libraries, Archives and Records, in the Place Directorate. The service supports and drives the efficient organisation of the council's information assets in whatever format. It takes a co-ordinated approach with other information-related services towards good information governance.

1.6 This policy sets out a lifecycle approach to records management, defining what is necessary at each stage to produce high-quality records. It outlines the expectations for all employees in managing information effectively and the responsibilities of different groups that directly support implementation of this policy. It will be supported by operational procedures.

2. Who this policy applies to

2.1 All employees, casual and agency workers, members, volunteers, contractors, partners, consultants and service providers are responsible for appropriately managing and storing the information they create and receive as part of council business.

2.2 **All employees, casual and agency workers, volunteers and contractors**

- Take personal responsibility for the effective management and protection of information

- Create full and accurate records of their work, inputting data and naming files in such a way that they can be easily accessed and understood by future colleagues
- Store information in shared locations that are accessible to colleagues and partners who are authorised to access it
- Keep sensitive and confidential information secure when not in use and do not leave it visible on an unattended desk
- Be aware of who can see the information on laptop screens and where possible, move to a more private space when working on very sensitive information
- Lock computers (press Ctrl+Alt+Del or Windows Key + L) when away from workstations for any reason
- Retain records until they have reached the end of their retention period as set out in the Dorset Council retention schedule
- Only destroy records after approval from the relevant Information Asset Owner, when records are no longer required and do not have value to Dorset History Centre
- Ensure information they have created, received or been responsible for in the course of their work remains accessible when leaving their role or the Council

2.3 **Members**

- Complying with this policy when acting as a Member of the Council e.g. sitting on a committee. When acting as a representative of residents of their ward, Members are individually responsible for the processing of personal data.

2.4 **Senior Information Risk Owner (SIRO)**

- Dorset Council's SIRO is the Corporate Director (Legal & Democratic Services)
- The SIRO is responsible for information risk within the Council and must ensure that effective records management policies and processes are in place.

2.5 **Information Asset Owners (IAOs)**

- Dorset Council's IAOs are Service Managers or equivalent roles.
- Assess and mitigate risks to information, for example the likelihood of a legacy system storing records becoming unusable
- Keep service and management records for as long as is necessary according to the Dorset Council retention schedule, and not longer, unless there is a genuine business reason
- Authorise records' disposal according to this policy and related procedures
- Update the Records Management service about organisational change and personnel moves that affect centrally managed records

2.6 **All managers**

- Take all reasonable steps to ensure that records management policies and procedures are followed by users
- Ensure appropriate resources exist to fulfil responsibilities for managing information

2.7 **Project managers**

- Take responsibility for managing project information from the start to the finish of a project
- Close down Teams (and private channels), ensuring that business and project information is migrated to a suitable place for continuing retention
- Transfer evidence of major projects to Dorset History Centre

2.8 **Contract managers**

- Ensure that third parties and partner organisations understand their obligations in receiving, handling, storing, disposing and returning information in the course of executing their contracts and agreements.

2.9 **Records Management Service**

- Promote a culture of good records management practice and raise awareness of records management issues
- Develop records management procedures and practices such as retention schedules, classification schemes and metadata schemas
- Advice users on their responsibilities and implementation of the policies
- Provide training and guidance
- Assessing records management compliance through oversight of all information storage locations and collection and reporting of metrics to demonstrate how information is being managed in practice

2.10 **Dorset History Centre**

- Preserve, protect and make available information from Dorset Council that has been selected for permanent preservation

3. Policy details:

The following are key concepts and principles from best practice standards, from which records management procedures will be developed.

3.1 **Overarching records lifecycle**

- Managing records effectively is essential to the efficient running of an organisation. Information must be proactively and consistently managed from creation or receipt, through active use, collaboration and maintenance, to disposal either by destruction or transfer to Dorset History Centre.
- Information created, received and maintained during normal daily business activities belongs to the Council.

- All recorded information including documents, data and records are subject to this policy. This includes information relating to external services and internal supporting services such as HR, Finance, and Property.

3.2 Creating information

- Create, keep and manage information that fully documents and enables the effective delivery of services
- Information must be named in such a way that it can be easily found by others now and in the future – with clear, meaningful and consistent titles and descriptive metadata (data about administrative context and relationship with other records) where required.
- To be considered authoritative evidence, records must have the following characteristics:
    - Authenticity: the record is what it claims to be and has not been tampered with. It can be relied on as evidence, for example in court.
    - Reliability: the contents of the record can be trusted as a full and accurate representation of the Council's activities.
    - Integrity: the record is protected against unauthorised changes, any changes are clearly indicated and have an audit trail.
    - Useability: the record can be found, used and understood as needed.
- A single version of the truth should be maintained, which is shared and reused between service areas. Avoid creating or keeping duplicates of information.
- Where emails or chats form evidence of a decision, the decision should be captured outside of the messaging system and not kept in a personal inbox or private chat.

3.3 Storing digital information

- Information that supports day-to-day business must be stored in SharePoint – including those sites that underlie Teams – unless there is an appropriate business system that has the capability to attach documents. As far as possible, SharePoint is the main corporate system for unstructured information, including Office documents, pdfs and images.
- OneDrive must not be routinely used to store Council information, except line management information and early drafts not ready to be shared more widely. Work information shared from an individual's OneDrive must be moved to SharePoint, where permissions can be set and monitored by the Team Owner.
- New business systems and SharePoint sites holding documents should be designed and configured to store records with metadata (additional information about your files) proportionate to their value. This supports their authenticity and integrity and helps each record to be understood.

See section **below on organisational and technological change** for more information on requirements for new systems.

- Legacy information will continue to be stored on shared drives in the short-term. A service design project is creating processes for a managed and consistent transfer of files from network drives to SharePoint, or their deletion in accordance with Dorset Council's retention schedule.
- Information must not be stored on device hard drives, on portable media e.g. USB drives, or sent to personal email or cloud storage.
- Digital continuity must be considered for the systems and formats used to store digital records. Information with retention periods over 10 years should be actively managed and considered for migration to the council's digital preservation system, administered by Dorset History Centre.

3.4 Storing hard copy information

- New paper records should not be created, except where this is required for evidential, historical or legal purposes.
- Paper records that are not being added to anymore and that are not accessed on a regular, monthly, basis must be transferred to the Records Management Unit (RMU).
- Physical records stored in the RMU and elsewhere must be controlled through a tracking system that documents their location and file movements.
- Paper records retrieved from the RMU must be promptly returned after use.
- Physical records should be stored in environmental conditions (stable temperature and humidity levels, adequate pest management and fire prevention are some examples) that protect them from deterioration. Long-term records and future archives should be stored in conditions conforming to BS 4971:2017 Conservation and care of archive and library collections.

3.5 Security

- Paper records and removeable media containing personal data must be kept in lockable storage or secure filing rooms, with access keys also held securely.
- Paper records must be destroyed using confidential waste bins at Dorset Council sites. Never destroy confidential material using non-council (i.e. home or a third party location) waste facilities.
- Records awaiting destruction must be stored securely.
- Documents stored on electronic systems should be deleted when no longer needed for business or retention purposes, including back-ups, and not overwritten.
- When information is destroyed, all copies of the information should be destroyed at the same time (both digital and physical). Information cannot

be considered to have been completely destroyed unless all copies have been destroyed as well.

3.6 Organisation and control

- All systems and records must have designated owners throughout their lifecycle. If an owner is not separately identified, the service manager as Information Asset Owner is responsible.
- All records must be referenced in Dorset Council's Information Asset Register, a simple catalogue to help us understand and manage our information assets and the risks to them. For more information, see the Information Governance Policy.
- Information requirements for the Council's most valuable records should be referenced in business continuity plans and risk registers.

3.7 Access and sharing

- Information should be stored with open access to view records unless there is a need to restrict it, for example due to the need to protect personal or commercially sensitive data.
- Designated owners of systems must ensure that appropriate technical and organisational measures are put in place to protect records from unauthorised access and accidental loss or destruction. This will vary according to the nature and purpose of the system but includes anything from ICT technical controls to service procedures for maintaining permissions, such as dealing with new starters and leavers.
- Team Owners must manage the membership and permissions for their Teams workspace.
- Access must be removed promptly from individuals who have moved to a different role.
- Users should share information from SharePoint via links. This helps to mitigate the risks from creating duplicates that need to be deleted, and working with outdated information.
- Users must report data breaches immediately to the Information Compliance Team.
- Where information is shared with or created by third parties, GDPR compliant contracts must set out what information is shared, how it can be used, how it should be handled and arrangements for its security and safeguarding.

3.8 Retention and disposal

- Information will be retained only for as long as it is required to support business need, legal obligations, for reference or accountability purposes, or to protect legal and other rights and interests.
- Dorset Council's retention schedule lists the records created by the Council and the minimum amount of time they must be kept before destruction or transfer to Dorset History Centre for permanent preservation.

- All information that is beyond its retention period must be approved for disposal without delay.
- The Records Management Service manages the regular and systematic disposal of records including the process of gaining authorisation for records disposals from Information Asset Owners.
    - This currently only applies in the Records Management Unit (RMU).
    - The corporate Records Management Project will bring all paper records into the tracking system used by the RMU.
    - The service design project will develop a process for systematically disposing of information from SharePoint and elsewhere in M365.
- Destruction must be performed securely and irretrievably.
- Disposal of information must be documented to provide evidence that the destruction took place in accordance with the retention schedule and with appropriate authorisation.
- Information that is due for disposal, but related to an ongoing information request, legal proceeding, regulatory investigation, audit or public inquiry must not be destroyed until the matter, including any complaint or appeal, has been closed.
- Personal data must not be kept for longer than you need it.
- Outside of the Records Management Service's disposal process local arrangements may allow destruction of records, where:
    - Authorisation is gained from the Information Asset Owner. If the information has no current owner, the closest manager to the function is responsible for the decision, with advice from the Records Management Service.
    - Destruction is documented, either automatically by an audit trail, or manually by completing a destruction log, which must be forwarded to the Records Management Service.
    - Information that is trivial, needed for a limited period and not included on the retention schedule should be destroyed as soon as no longer required as part of routine housekeeping.
    - Records representing the corporate memory of Dorset Council and the cultural heritage of Dorset, that are suitable for permanent preservation, should be offered to Dorset History Centre (contact archives@dorsetcouncil.gov.uk)

3.9 Organisational and technological change

- Records management requirements must be routinely factored into ICT planning, procurement, implementation and decommissioning.
- Digital continuity considerations should be included in Digital and Change processes.
- Specific records management requirements for new systems include:
    - The ability to capture metadata about context and interrelationships so that retention and disposal can be applied by groups of records
    - The ability to configure a systematic disposal process that only allows authorised users to review and make disposal decisions
    - The ability to generate an audit trail on which occasions records have been seen, used, amended and deleted

- The ability to migrate data in order to ensure the completeness, availability and usability of information after the system has been decommissioned. Where necessary for long-term preservation, this includes extracting and transferring data to a digital preservation system.

3.10 **Protective marking and handling**

- Protective marking is a standardised method of highlighting which information needs additional care to protect it. Dorset Council uses the Government Security Classifications policy to classify information.
- All information created by the Council is classed as Official. There is no requirement to formally label Official information.
- Some information with extra requirements for protection must be protectively marked with the descriptor 'Official – Sensitive'. This only applies where sensitive information could have damaging consequences if lost, stolen or published, and the sharing warrants that handling requirements need to be reinforced. It is not necessary to protectively mark routinely shared work within a team.

3.11 **Evidential weight**

- Physical records that are scanned with the intention of destroying the original should be scanned in such a way that the scanned image is an authentic copy.
  Dorset Council intends to comply with BS 10008 Evidential Weight and Legal Admissibility of Electronic Information and will produce procedures covering image quality, indexing and quality control.

4. Learning and skills development

4.1 As all Council employees are involved in creating, using, and maintaining records it is vital that everyone understands their records management responsibilities as set out in this policy.

4.2 Training on records management will be provided to all employees. The programme of training should include inclusion in new starter inductions and regular refresher sessions to remind staff of their responsibilities.

4.3 This policy will be supported by procedures and learning materials.

4.4 Briefings will be provided to teams on request and regular reminders on records management topics shared through corporate communication channels.

5. Monitoring compliance

5.1 This policy will be supported by projects and strategies that will have their own monitoring and governance routes.

5.2 Records management performance will also be monitored at a service level and areas of concern raised with directorate management teams.

5.3 Non-compliance with this policy may result in the Council being put at risk of legal challenge, service users being put at risk, colleagues being inconvenienced with their time wasted, and Council resources being wasted.

Actions or neglect leading to a breach of this policy by an individual employee could result in disciplinary action.

6. Policy approval and review

6.1 Monitoring of this policy will be undertaken by records management staff on a regular basis and reported to the Information Governance Board. It will be reviewed in September annually, or after major technological or organisational changes, to ensure it continues to meet the requirements of the Council and the current legislation.

Annex A

Related policies :

- Information Governance Policy
- Data Protection Policy
- Data Breach Policy
- Individual Rights Policy
- Data Protection Impact Assessment Policy
- Information Security Management Policy and related standards and protocols
- ICT Security Strategy
- ICT Security Management Policy
- ICT Acceptable Use Policy

Annex B

This policy is written with reference to the following legislation and standards:

- Freedom of Information Act 2000 and the Code of Practice on the Management of Records under Section 46 of the Act
- General Data Protection Regulation and Data Protection Act 2018
- Environmental Information Regulations 2004
- ISO 15489 Records Management
- British Standard 10025 Records management - Code of practice
- BS ISO 16175-1 Processes and functional requirements for software for managing records
- BSI BS 10008 Evidential weight and legal admissibility of electronic information
- BS 4971:2017 Conservation and care of archive and library collections