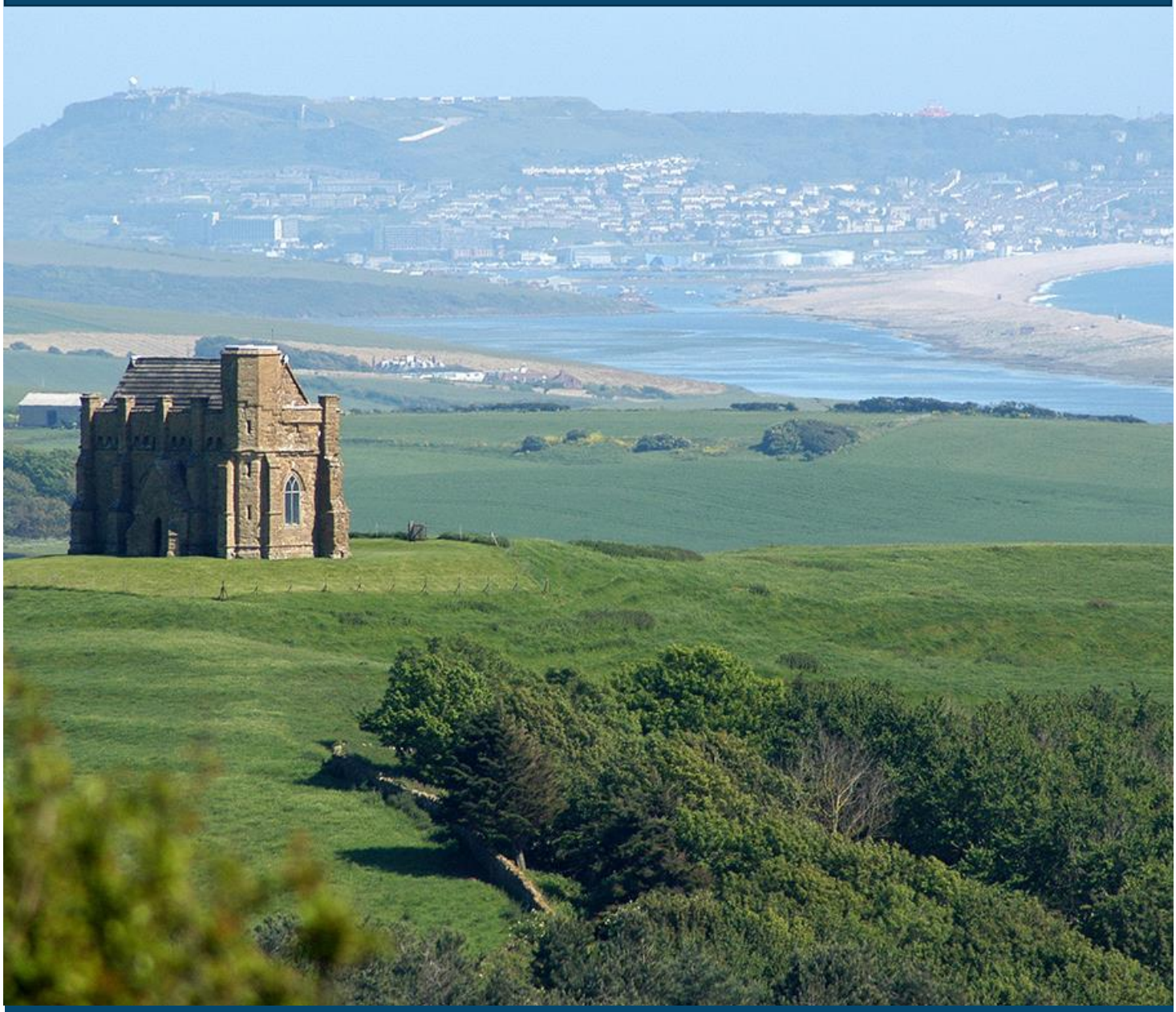
Records Management Policy



Dorset Council

Version control			
Version	**Authors**	**Date**	**Changes**
0.1	Kate Watson, Shannon Parsons	08/11/2024	First draft submitted to IG Operational Group
0.2	Kate Watson	03/01/2025	Updated wording for clarity

Records Management Policy

What this policy is for

This policy explains how to manage information in a simple and consistent way, following accepted standards for records management.

The policy applies to:

- all information created during work, which belongs to the council
- all types of information, whether digital or physical (paper)
- all employees and contractors who work with council information

Good records management is everyone's responsibility. This policy tells you what you need to do to manage and protect information properly.

If you manage a service, you have extra responsibilities as an **Information Asset Owner (typically service managers or heads of service)**. These are listed in the Information Governance Policy and throughout this policy. Managers should implement these requirements based on their service's needs and the level of risk involved.

The records management function helps the council manage information throughout its lifecycle, from creation to disposal. This ensures we meet service needs, compliance requirements, and public and partner expectations. The Records Management team provides advice and support on how to follow this policy.

Why good records management matters

Good records management helps our colleagues, customers, and the whole organisation work better.

It means storing information in an organised way and keeping evidence of what we have done. This ensures information:

- is easy to find and use for day-to-day tasks
- is secure and protected based on its importance
- can be used to improve and innovate
- provides reliable evidence when needed
- is safely destroyed when no longer required, saving space and reducing environmental impact

Managing information well is key to effective data protection and information security. This policy follows the rules in the **Freedom of Information Act 2000 (FOIA)** and the **Data Protection Act 2018**, including the **General Data Protection Regulation (GDPR)**.

Records management is part of the Information Governance framework and supports compliance with related policies.

Policy statement

Dorset Council recognises that information is valuable and managing it is an important part of our work.

We manage information based on the lifecycle concept, which describes how information goes through different stages: creation, use, maintenance, and eventually disposal or preservation. Each part of this policy describes a key goal for managing information across its lifecycle. There are clear steps for everyone to follow, and extra responsibilities for Information Asset Owners to include in their service management.

The main requirements of this policy are to:

1. manage information assets according to their value and risks
2. create complete and reliable evidence of activities
3. implement fit-for-purpose systems to manage information throughout its lifecycle
4. dispose of digital and physical information in a planned and authorised way
5. reduce areas of information inefficiency and risk

Manage information assets according to their value and risks

Information is a valuable resource and we need to manage it responsibly.

All information users need to:

- take personal responsibility for managing information with care, and follow the law and policies that apply to it
- only use council systems for storing digital information, and council buildings for physical records
- protect information when taking it off-site or transferring it between locations
- keep your desk clear of sensitive information and lock your screen when you are away from your desk, both in the office and when working remotely
- be careful not to wrongly share confidential information – see the Code of conduct for employees

The council follows the Government Security Classifications Policy. Security classifications indicate how sensitive information is, based on the potential impact from compromise, loss or misuse.

The classifications for our information are:

- **Official - Public:** information in the public domain or cleared for publication, that can be shared without restriction

- **Official:** information that must remain protected but can be shared internally or externally within existing controls. This is the majority of the information we use in council business.
- **Official - Sensitive:** information that must remain protected and, due to a greater risk of damage to the work or reputation of the organisation and individuals, needs authorisation from the Information Asset Owner to share. Official - Sensitive information must have a clear marking that is visible to anyone using or receiving the information.

All information users need to:

- protectively mark information when it's created, shared or received
- think about how sensitive information is when deciding how to share or store it
- only share sensitive or personal information externally as part of an agreed business process, approved by your Information Asset Owner
- until this policy is fully in place, assume that all information needs to be protected, whether it is classified or not
- if you suspect information has been lost, stolen, accessed without permission or misused, report it immediately to your manager. Report a data breach if the compromised information contains personal data
- be aware that emails, messages and files are monitored to detect and prevent data breaches, unauthorised leaks, or unwanted destruction of sensitive data

Information Asset Owners have extra responsibilities to:

- keep track of where information is stored and register it on the Information Asset Register (IAR)
- keep your retention policies on the retention schedule up-to-date and contact Records Management to make changes
- review risks to your information and include them in your risk register entries and business continuity plans
- ensure there is secure access to information for remote working and permanent home workers
- consider the need for secure storage when moving office space
- ensure that information is protected appropriately, especially when sharing it
- lead by example, promote good security behaviours and make sure your team apply security classifications and markings correctly

Create complete and reliable evidence of activities

Creating accurate and reliable records helps us make good decisions and supports efficient services.

All information users need to:

- make formal records, such as case notes, as soon as possible after the event
- record the facts clearly, including what happened, when, why, and how. Provide enough context to make the activity understandable.
- give files clear, meaningful and consistent titles so they can be easily found by others in future
- save documents in shared locations that you have checked are accessible only to authorised users

Information Asset Owners must make sure that reliable records are created as part of business processes. Your extra responsibilities are to:

- make sure new starters are trained on how to create and access information
- set up processes for transferring knowledge when staff leave the team, and removing access when staff change roles internally
- clearly define in your procedures where and how documents should be stored to avoid duplication and inconsistent storage. This includes ensuring that shared storage is used rather than individual OneDrive accounts.
- create standard rules for naming files across your team
- think ahead about which digital information needs to be kept for more than 10 years. You need to ensure it is stored correctly to be reliable evidence and to be accessible in the long-term.
- set up quality control in scanning projects, to ensure scanned images are accurate copies before the originals are destroyed. Only keep the originals if there is a genuine business or legal need.

Implement fit-for-purpose systems to manage information throughout its lifecycle

All information users need to understand their role in managing information at each stage of the lifecycle:

- create – save information with a clear name, and protectively mark it
- use – store information so the right people have access while in active use
- maintain – keep your storage areas organised. Update information with important details like dates when closing a case, to inform its management over time.
- dispose – when information reaches the end of its agreed retention period, follow the rules defined in the retention schedule
- preserve – be aware that some information is kept permanently and contact Dorset History Centre about potential archives

Information Asset Owners must ensure that information is available and managed throughout its full retention period. This involves designing systems and storage to meet information requirements and automating controls where possible. Your extra responsibilities are to:

- define usability, security, retention and long-term preservation requirements when purchasing or upgrading systems, based on the ICT general requirements
- build the right features into systems. Make sure your information systems and storage can:
    - track metadata containing important details about each piece of information and its relationship with other data
    - add protective markings to documents automatically based on location or document template
    - calculate retention periods when information is created, or when triggered by specific events
    - prevent information from being changed or tampered with
    - store information that needs to be kept over 10 years in the council's long-term digital preservation system, contact Dorset History Centre
    - put in place permissions that share information no wider than necessary for business needs
    - change permissions where needed, at different stages of the lifecycle
    - export data or migrate to new systems at the end of contract
- transfer paper records to the Records Management Unit (RMU) when no longer in active use
- ensure that paper and other physical records are stored in environmental conditions that protect them from damage

Systems that are only accessible to individuals, such as individual email accounts, Teams chat and OneDrive are not fit-for-purpose locations for storing council records.

We understand it may take time to implement these changes as new systems are put in place. Information Asset Owners can ask for support from the Records Management team and other information governance professionals to design and implement the right solutions.

Dispose of digital and physical information in a planned and authorised way

Destroying information when it's no longer needed helps save resources and reduces the risk of fines and reputational damage due to data protection non-compliance.

The Records Management team supports Information Asset Owners to manage the planned disposal of digital and paper information, following the retention schedule. This defines how long to keep information before it's destroyed or transferred to the Dorset History Centre. Disposal of information should be properly documented.

All information users need to:

- only destroy council information when authorised to do so by your Information Asset Owner
- contact your Information Asset Owner if a change or addition is needed to the retention schedule
- destroy trivial information that is only needed temporarily, as soon as no longer useful
- look out for unique records that are important to the council's history or local heritage, and offer to Dorset History Centre before they are destroyed

Information Asset Owners are responsible for approving the disposal of information relating to your service that has passed its retention period. This is usually done by groups of records in bulk, rather than item-by-item. The Records Management team will assign decisions about legacy or 'orphaned' information to the most relevant manager. Your extra responsibilities are to:

- approve the destruction of groups of records based on the retention schedule. You only need to look at individual files if there's an anticipated legal or business reason to keep them longer.
- only pause or extend retention when there is a valid reason, such as statutory information request, legal proceeding, regulatory investigation, audit or public inquiry
- oversee the retention and disposal of information in your locally managed systems
- transfer information that needs to be permanently preserved to the Dorset History Centre when it's no longer in active use

Reduce areas of information inefficiency and risk

By following this policy, and keeping only what's necessary, we can use our resources more efficiently, be better at knowledge-sharing and make sure our corporate memory is preserved. Well-managed information also supports accountability and builds community trust in the council's services.

There are areas of information management that could be more efficient and safer, especially where we are keeping information too long and sharing it too widely. The

Information Asset Register can be used as a tool to understand what information the council holds, how valuable it is, and where improvement is needed.

Information Asset Owners are responsible for reducing information risks and creating a culture that values, protects and uses information for the public good. Your extra responsibilities are to:

- review your information assets regularly, and where they don't meet business needs make plans to fix the issues
- keep site and system owners, and the Records Management team, informed about staffing changes that affect access to information
- carefully balance the risks when dealing with large quantities of legacy information. There are privacy concerns from keeping it too long and potential business impact from destroying it too soon.
- include information management requirements in change management, procurements, system upgrades and migration
- ensure the long-term usability and accessibility of required information when decommissioning systems

Information Asset Owners can get support from the Records Management team and other information governance professionals.

Roles and responsibilities

All employees:

- are personally responsible for storing, managing and protecting the information you create and use
- must keep records that are complete, reliable, and easy to find and understand by future colleagues
- understand the value of the information you hold, its security classification and how long it needs to be kept

Information Asset Owners:

- set up processes to make sure that this Records Management Policy and related procedures are followed in your team

Senior Information Risk Owner:

- overall accountability for ensuring that effective systems and processes are in place to address the Information Governance agenda, including information and records management.

Strategic Information Governance Board:

- chaired by the Senior Information Risk Owner (SIRO), this Board and its operational working groups monitor compliance with this policy

Archives and Records service:

- promote good information management practices across the organisation
- create and maintain records management tools like retention schedules, classification schemes and metadata schemas
- provide training, advice and support to individuals and Information Asset Owners about following this policy
- oversee how information is stored to monitor compliance with this policy
- ensure that information needing to be permanently preserved is selected and transferred to the Dorset History Centre at the appropriate time

Elected Members:

- when Elected Members access and process council information, they must follow this policy.

Enforcement

If employees don't follow this policy, either on purpose or through negligence, it will be investigated, and disciplinary action may be taken according to disciplinary procedures (and in line with the ICT Acceptable Use Policy and Code of Conduct for Employees).

Non-compliance may be reported to the Senior Information Risk Owner (SIRO) or the relevant information governance working groups.

Review

Policy owner: Corporate Director Transformation, Customer & Cultural Services

Policy contact: Data and Information Manager

Approvals: Operational IG Group, Strategic Information Governance Board

Date approved: 20/01/2025

Review date: January 2027

Implementation guidance and support

The Archives and Records service will provide guidance to support services to implement this policy. It is not intended to cover all scenarios, please contact the Records Management team for specific advice.

Appendix – relevant 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
- Government Classification Scheme
- Guidance 1.1 - Working at OFFICIAL
- 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