Audit and Governance Committee
27 April 2026
Annual Information Governance Report
For Review and Consultation

Cabinet Member:
Cllr N Ireland, Leader of the Council, Climate, Performance and Safeguarding

Senior Leadership Team:
J Mair, Director of Legal & Democratic

Report author and job title: Marc Eyre, Service Manager for Assurance
Email: marc.eyre@dorsetcouncil.gov.uk

Statutory Authority: Information Commissioner

Report status: Public (the exemption paragraph is N/A)

1. Executive summary

1.1. This is the fourth Annual Information Governance Report, to be presented to the Audit and Governance Committee. The aim of the report is threefold: i) to provide an update on information governance activity; ii) to provide assurance that arrangements are fit for purpose; and iii) identify areas of improvement and focus for the forthcoming year.

1.2. The report is split into two sections, aligned to the Data and Information Management theme in the risk register. Section one focuses on those strategic risks that are reported to committee. Section two extends to cover the more operational risks that have been referenced previously within annual reporting to this committee, and provide a holistic view of the Council's information governance risk.

1.3. For each risk an update has been provided on the current position (including progress on any outstanding audit actions), key activities during 2025/26, and actions identified for 2026/27 (where relevant) to bring the level of risk down to a perceived acceptable level, in line with the Council's risk appetite.

1.4. The Strategic Information Governance Board's remit (and previous Annual Reports) includes cyber risk. This year, cyber risk is being reported separately on this agenda, and therefore excluded from this paper. That paper proposes a separate annual reporting process on cyber risk.

1.5. At its January meeting, the Committee requested an update on the actions identified during SWAP's Data Maturity audit, and in particular sought assurance over management response to priority 1 and 2 actions. This has been addressed within this report, linked to appropriate risk register entries (strategic risk 22; operational risk 326).

1.6. On consideration of last year's report, there was particular focus from committee on performance on information requests (operational risks 44 and 50); training compliance levels (strategic risk 39) and data breaches (operational risk 49), including more detail on the type of breaches.

2. Recommendation(s)

2.1. To note the 2025/26 activity and focus for 2026/27

3. Reason for the recommendation(s)

3.1. To ensure that information governance is embedded and effective across Dorset Council.

4. Strategic Information Governance Risks

4.1. This section covers the latest position on the following strategic risks linked to the Data and Information risk theme:

ID	Risk Title	Risk Rating
22	Due to a failure to effectively migrate and manage digital information, Dorset Council may be unable to access or trust its data, leading to disruptions in business operations and decision making	High
29	Due to insufficient business continuity planning and testing, one or more service may fail during a disruption, leading to disrupted service delivery	Medium
39	Due to lack of compliance with mandatory NHS Data Security and Protection Toolkit requirements Dorset Council may lose access to health data impacting its ability to deliver integrated care and strategic partnership objectives	Medium
91	As a result of a successful cyber-attack, Dorset Council's IT systems may be compromised leading to a loss of service of data *[Covered within separate agenda paper "Protecting our council - cyber security risk management and future improvement plans"]*	Very High
92	Because of a disruption such as a power failure Dorset's ICT recovery may be delayed leading to operational disruption	High

Risk:	22	Due to a failure to effectively migrate and manage digital information Dorset Council may be unable to access or trust its data leading to disruptions in business operations and decision making.			
High	**Risk Owner(s)**	Sam Johnston / Kate Watson / Cassandra Pickavance / Emma Blowers (Archives and Information Management)	**Reviewed**	16/03/26	

Current Position (including audit action status)

The significant volumes of data held on network drives have a direct impact on the Council's resilience to a cyber incident, data protection compliance, and its ability to achieve best value from the Microsoft 365 digital platform.

Much of this data was inherited from predecessor councils and, as organisational structures and responsibilities have changed over time, information ownership has become less clear. Under the Information Governance and Records Management policies, services are responsible for maintaining their information, including keeping files organised and deleting information in line with agreed retention periods.

As services have increasingly moved to saving current work in Microsoft Teams and SharePoint, and away from legacy network drives (for documents not held within core business systems), there is a growing risk that large volumes of information are retained without a clear purpose, owner or retention rule, and equally that valuable information could be 'left behind'.

Greater use of Microsoft Purview capabilities to apply automated retention and disposal controls to digital information is planned. However, the effective use of automated retention is dependent on well-designed SharePoint structures, clear information ownership, and accurate classification of content. Until digital information is migrated into agreed structures, there is limited ability to rely on automation to control information growth and manage risk.

During the past year, the Records Management (RM) team has worked with ICT and user adoption colleagues to pilot a structured approach to digital migration. The pilot confirmed that effective migration requires consistent engagement from services and sufficient capacity to deliver this activity at the pace and scale required.

A proposal to implement structured storage in Microsoft 365 using SharePoint has been agreed through the Design Authority. This approach has also been recognised through the SWAP Data Maturity Audit, which includes an action to link files to Information Asset Owners, classify content and apply retention labels to migrated information in order to prevent a similar build-up of unmanaged data in future.

However, while structures and governance are being put in place, there is currently no dedicated delivery capacity to implement migration at scale, and therefore limited assurance that the risk is currently being reduced at a corporate level. Existing Records Management, ICT and user adoption resources are small and already supporting multiple corporate priorities, which limits progress beyond pilot and design activity.

A project manager has been assigned on a short-term basis to design the next phase of work, however, this resource is time-limited and focused on planning rather than delivery and does not in itself provide a mitigation for the underlying risk. The risk remains active pending agreement on delivery capacity and continues to be monitored by the services involved.

Active service involvement remains essential to designing and maintaining effective information structures within SharePoint.

Key Developments 2025/26

- Design Authority approved proposal to move from legacy storage, including network drives, into a structured SharePoint environment so that information can be actively managed and automated.
- Project manager assigned to plan next phase, although currently resourcing beyond first phase of 2 months is uncertain.
- Public Digital review of DC's cyber preparedness has complemented the approach proposed in the digital records project.

Key Actions for 2026/27

- Respond to any recommendations that may be made by Public Digital, following cyber review work
- Design the next phase of work, building on the outcomes of the pilot activity. The detailed scope, outcomes and delivery timescales are currently being developed and will be informed by further assessment of the resources required.
- Continued work to develop tools that improve visibility of file storage and support services in making proportionate decisions about what information should be retained, migrated or disposed of.
- Delivery will require active engagement from services, reflecting their responsibilities under the Information Asset Ownership model, alongside central coordination and specialist support.

Risk:	29	Due to insufficient business continuity planning and testing, one or more service may fail during a disruption, leading to disrupted service delivery			
Medium	**Risk Owner(s)**	Marc Eyre / Georgie Connelly (Assurance – Emergency Management & Resilience)	**Reviewed**	31/03/26	

Current Position (including audit action status)

The business continuity process is facilitated by the Emergency Management and Resilience Team (EMRT), but responsibility for specific response action cards rests with the individual services, with ownership at Service Manager and Heads of Service level. A key performance indicator is reported annually to Senior Leadership Team and Audit and Governance Committee, as part of annual reporting circa July.

A SWAP internal audit was initiated during 2024/25 to respond to concerns raised by the EMRT around the extent that action cards were maintained. This identified a number of P1/2 findings, which prompted a revision of the business impact analysis (BIA), critical services and critical systems. This was signed off by SLT, alongside a review and update of the business continuity framework. The BIA review will be undertaken annually, moving forward. There are no outstanding audit actions.

Testing of plans is key, and to support this, a number of mini exercises have been developed, to support teams in challenging the effectiveness of their plans against a range of business continuity scenarios. A number of service level exercises have also been held across the Place Directorate. However, it is recognised that there needs to be periodic whole authority testing, which is built into 2026/27 plans.

Key Developments 2025/26

- Sign off of the revised Business Impact Analysis and supporting critical services/systems list by SLT;
- Roll out of key performance indicator on number of services that have reviewed and updated plans;
- Revised business continuity framework;
- Ongoing development of business continuity “exercise on a page” scenarios.

Key Actions for 2026/27

- Respond to any recommendations that may be made by Public Digital, following cyber review work;
- Annual review of business impact analysis with Senior Leadership Team;

- Ensure that business continuity arrangements reflect change of working models following restructure/transformation (including hub models);
- Develop and deliver whole authority business continuity exercise.

Risk:	39	Due to lack of compliance with mandatory NHS Data Security and Protection Toolkit requirements Dorset Council may lose access to health data impacting its ability to deliver integrated care and strategic partnership objectives			
Medium	**Risk Owner(s)**	Marc Eyre / James Fisher / Alex Barrett (Assurance – Information Compliance / ICT Cyber Security)	**Reviewed**	31/03/26	

Current Position (including audit action status)

Access to health data sets are governed by satisfactory completion and approval of the NHS Data Security and Protection toolkit in June each year. Failure to achieve approval would have significant data access issues. At this point in time we are not fully compliant and marked as "approaching standards" in the 2025/26 assessment. There are four mandatory requirements that we do not currently fully meet:

- "a training needs analysis covering data security and protection, and cyber security, been completed in the last twelve months". This is mitigated by both data protection and cyber being mandatory modules, but does not reflect that some roles may require bespoke training. A draft matrix has been developed, pending approval. – this will be noted as "met" for June 26 return.

- "at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, in the last twelve months". Training rates have improved significantly but remain below 95%. As at 31 March they are 94% for data protection and 82% for cyber training (the cyber figure is distorted by the fact that courses are monthly, so delayed participation negatively impacts completion statistics). Despite this improvement, a process is being implemented to remove email access for officers that fail to complete training within a reasonable time period.;

- "a list of its suppliers that handle personal information, the products and services they deliver, and their contact details". This information is currently held across a number of datasets, and further work is required to consolidate this data into a comprehensive list, linking the applications to our Information Asset Register.

- "IT system suppliers having cyber security certification". Certifications are now required as part of the procurement process – this will be noted as "met" for June 26 return.

Key Developments 2025/26

- Development of the dashboard for cyber security training to improve data quality;

- Improved training rates. Reporting to committee in August 2025 highlighted data protection training at circa 89% (now 94%) and cyber 65% (now 82%).

Key Actions for 2026/27

- Implementation of controls for policing poor completion rates of training;
- Adjusting the key performance indicators for cyber training;
- Approval of training matrix;
- Ongoing roll out of Information Asset Register

Risk:	92	Because of a disruption such as a power failure Dorset's ICT recovery may be delayed leading to operational disruption		
High	Risk Owner(s)	James Ailward, Head of ICT Operations	Reviewed	16/02/26

Current Position (including audit action status)

Resilience for critical services hosted by the Council, including duplicated services operating from multiple data centres.

Service continuity and exercise response processes are managed by an experienced team and this will be reviewed as part of a set of new exercises to provide assurance on its outcomes.

Service continuity testing has resumed, proving assurance that the other controls in place work as intended.

Key Developments 2025/26

- Limited testing on key applications took place easter 2025, this is the foundation for twice yearly regular testing to maintain and improve the Councils posture.

Key Actions for 2026/27

- Twice yearly testing.

5. Operational Information Governance Risks

5.1 This section covers the latest position on the following operational risks linked to the Data and Information risk theme:

ID	Risk Title	Risk Rating
16	Insufficient indexing of Dorset Council's records in all formats prevents accessibility and retrieval of data for statutory reporting and scheduled disposal preventing Dorset Council from becoming a more responsible customer focussed council	Low
20	Failure to sustain a programme of digital preservation thus risking impairment and loss of the corporate memory, reputational damage and breach of statutory codes	Medium
27	Loss of Dorset Council's physical records causes disruption to business operations preventing Dorset Council from becoming a more responsive customer focussed council	Medium
28	A fraudulent information request is made resulting in sensitive information being provided to the wrong person	Medium
35	Insufficient policies and procedures aimed at helping the organisation to comply with its data protection obligations results in a poor information compliance culture	Medium
41	Unable to sustain Assurance Service due to prolonged pressures (increasing caseloads etc, changing legislative demands and gaps in staff capacity)	High
43	Inadequate leadership and oversight of data protection activities at a strategic and operational level results in poor information compliance culture	Low
44	Inadequate compliance with individual rights under data protection law	Low
45	Insufficient transparency around Dorset Council's data processing activities	Medium
47	Contracts and data sharing arrangements do not comply with statutory data protection standards	Medium

48	Failure to complete data protection impact assessments prior to commencing or changing high risk data processing activities	Medium
49	Failure to detect, investigate, risk assess, record and respond to data breaches	Medium
50	The Council does not adhere to the Information Commissioner's Code of Practice in relation to the Freedom of Information and Environmental Regulations requests, resulting in regulatory enforcement and reputational damage	Low
52	Data loss / leakage by internal staff / leavers	Medium
55	Failure to comply with Regulation of Investigatory Powers Act 2000 or other covert surveillance legislation	Medium
117	As a result of inaccurate business intelligence, uninformed decision making may take place at a strategic level leading to a failure to deliver the Council's services and/or priorities effectively	Medium
326	Because information management policies are not consistently applied controls over how information is stored and maintained may not be followed resulting in unnecessary data growth, duplication, security vulnerabilities and increased operational costs	Medium

Risk:	16	Insufficient indexing of Dorset Council's records in all formats prevents accessibility and retrieval of data for statutory reporting and scheduled disposal preventing Dorset Council from becoming a more responsible customer focussed council			
Low		**Risk Owner(s)**	Sam Johnston / Kate Watson (Archives and Information Management)	**Reviewed**	23/12/25

Current Position (including audit action status)

Insufficient indexing of records presents a risk to the Council's ability to find information efficiently, meet statutory reporting and information access requirements, apply correct retention, and securely manage access to sensitive data. This is particularly significant for services holding large volumes of complex case records

For Children's Services records, a directorate-funded Children's Records Project has provided dedicated, fixed-term capacity to address long-standing issues with the indexing of paper records. This focused support has delivered significant improvements in the quality and consistency of record indexing, strengthening confidence in information ownership, access controls and retention decisions.

However, the project resource is currently funded on a fixed-term basis, concluding in December 2026. It is anticipated that, without continuation of this capacity, a substantial body of work will remain incomplete, limiting the ability to sustain progress and extend the same level of compliance and assurance across all Children's Services records.

Across other services, inconsistent indexing of legacy paper records is a contributing factor to significant backlogs of paper records being kept for longer than their scheduled retention periods. Where records are insufficiently indexed, services find it more difficult to make retention decisions, reducing the effectiveness of the self-service model.

Key Developments 2025/26

- Children's Records Project has preserved data from closed services including The Cherries residential home and Blandford Children's Centre Nursery (including Oscars Out of School Club)
- The project has improved data for over 60,000 records held in managed storage so that the correct retention dates can be applied, and significant quantity of confidential waste destruction has been carried out.

Key Actions for 2026/27

- Supporting the review and removal of records from the County Hall basement – transfer to RM for improved searchability and retention management. Seeking consistency of approach across council departments to RM post-LGR.
- Proposal to adopt a tiered service model to allow more focused for services with the largest or highest-risk backlogs of paper records retention decisions
- Making the case to identify additional resourcing for ongoing needs of records of Children's Services.

Risk:	20	Failure to sustain a programme of digital preservation thus risking impairment and loss of the corporate memory, reputational damage and breach of statutory codes			
Medium	**Risk Owner(s)**	Sam Johnston (Archives and Information Management)	**Reviewed**	11/02/26	

Current Position (including audit action status)

Proprietary software Preservica has been used by the Archives service for over a decade to protect digital information with permanent and long-term value. Significant volumes of material have been ingested, including highly sensitive council records such as scanned adoption files, however much council material is kept in operational systems.

There remains an urgent need to align SharePoint architecture, information ownership and retention policies with digital preservation processes, so that records identified as having long-term or permanent value can be preserved seamlessly.

At present, this integration is not consistently in place. As a result, information may be at risk of loss, degradation or may be kept in unsupported formats.

Progress in this area is strongly dependent on the successful delivery of the wider digital file migration and information management transformation. This risk is therefore closely interdependent with Risk ID 22, which addresses the Council's ability to effectively migrate, manage and govern digital information currently stored across network drives and unmanaged Microsoft 365 locations.

Key Developments 2025/26

The digital records project (commenced March 2026) will, if resourced to completion, provide a mechanism for SharePoint and Preservica to link interoperably thereby facilitating the transfer of service-generated records into a permanent preservation environment. However, this is a major undertaking and will require prioritisation by services and additional resourcing for Records Management.

Communications about digital records project and need for services to review their information and delete or transfer to SharePoint has been undertaken.

Key Actions for 2026/27

Commencement of digital records project to transfer records from shared drives and prepare for decommissioning of the latter in May 2027.

Risk:	27	Loss of Dorset Council's physical records causes disruption to business operations preventing Dorset Council from becoming a more responsive customer focussed council		
Medium	**Risk Owner(s)**	Sam Johnston / Kate Watson (Archives and Information Management)	**Reviewed**	23/12/25

Current Position (including audit action status)

Dorset Council continues to hold physical paper records that remain essential to the delivery of some services and to meeting legal, regulatory and corporate memory requirements.

During the heavy rain this year, water leaks were identified within the Records Management Unit, the main corporate paper records store in County Hall. These incidents were proactively managed, with actions taken in collaboration with Property colleagues to protect records and better prepare for any future incidents. It is anticipated that the replacement of the roof at the front of County Hall will reduce the risk of future water ingress.

Records held within the Records Management Unit benefit from regular monitoring and conservation-approved processes. However, physical records stored outside of managed environments present a higher level of risk, as they are not routinely monitored for environmental conditions and may not be adequately protected or recoverable in the event of damage.

The recent incidents have reinforced the importance of appropriate centralised storage and the consistent application of records management controls in order to reduce the risk of information loss and service disruption.

Key Developments 2025/26

- Mitigation against water damage within RM stores by team has resulted in the need to move some files and to protect against further unpredictable leaks.

Key Actions for 2026/27

- Work relating to the above (and see Risk ID 16) is ongoing with Property colleagues and record owners.
- Service owners of records in the County Hall basement and other satellite outstores (including Westport House) have been encouraged to work towards transfer into RM custody to bring about a consistent, single approach to the management of paper records.

- There is uncertainty at time of writing as to how many records will be transferred from unmanaged locations and thus what the resourcing requirement for RM will be.

Risk:	28	A fraudulent information request is made resulting in sensitive information being provided to the wrong person			
Medium		**Risk Owner(s)**	Marc Eyre / James Fisher (Assurance – Information Compliance)	**Reviewed**	31/03/26

Current Position (including audit action status)
This risk forms part of the Councils fraud risk assessment. Under the General Data Protection Regulations individuals are entitled to receive copies of any documentation that an organisation holds about them. Before releasing this information, the Information Compliance team go through a process to check the identity of the requestor. The risk is identified as Medium, as the potential risk could be significant should the controls fail. However, the risk is managed down to a level acceptable to tolerate.
Key Developments 2025/26
None
Key Actions for 2026/27
None

Risk:	35	Insufficient policies and procedures aimed at helping the organisation to comply with its data protection obligations results in a poor information compliance culture		
Medium	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)

The portfolio of information governance policies and standards were initially developed by the Shaping Dorset programme and effective from day one of Dorset Council. Whilst a number of these policies have been reviewed and updated, others are significantly overdue review. A prioritisation schedule has been developed and is being managed by the Operational Information Governance Group. Policies are signed off by the Strategic Information Governance Board. This prioritisation has been based on the extent that the existing policy remains fit for purpose. A Senior Data Protection Analyst (12 month contract) commenced employment in August 2025 and part of their remit was anticipated to be the review and update of information compliance policy documents, however other pressures on the Information Compliance team have diverted this resourcing. Policies cover the range of information compliance, information management and cyber security, and are made up of the following (those overdue review are marked in red):

Information Governance	Data Quality	ICT Acceptable Use
Data Protection	Data Sharing	ICT Security Management
Data Breach	Records Management	ICT Security Strategy
Data Protection Impact Assessment	Use of Covert Surveillance	Artificial Intelligence
Individual Rights	Business Continuity framework	

Whilst not forming a recommendation, the prioritisation work on policy updates was referenced within the Data Maturity audit work.

Key Developments 2025/26

- Revised data breach reporting process (see risk 49)
- Development of new Data Protection Impact Assessment screening tool (see risk 48)

Key Actions for 2026/27

- Seek extension of temporary contract for Data Protection Analyst role
- Ongoing rollout of policy updates
- Review of ICT Acceptable Use policy, to reflect technological change

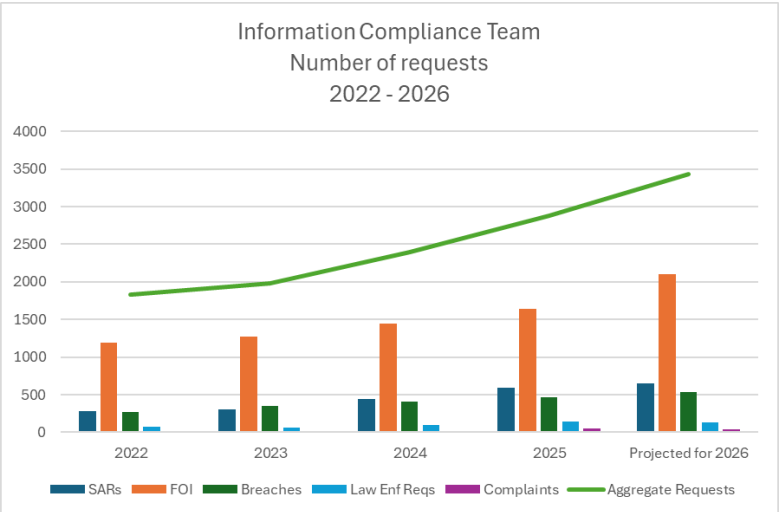
Risk:	41	Unable to sustain Assurance Service due to prolonged pressures (increasing caseloads etc, changing legislative demands and gaps in staff capacity)		
High	Risk Owner(s)	Marc Eyre (Assurance)	Reviewed	31/03/26

Current Position (including audit action status)

The Assurance Service contains a number of functions – Information Compliance; Complaints; Emergency Management and Resilience; Fraud/Governance; Police and Crime Panel. There are pressures across all teams, but for the purpose of this report, the focus is on the Information Compliance team. This small team of 10 ftes is managed by the Data Protection Officer, and includes responsibility for facilitating information requests (Freedom of Information; Subject Access Requests; Law Enforcement Requests); responding to data breaches; and strategic support to services in respect of compliance with Data Protection legislation.

Caseloads across the team have increased significantly:

	SARs	FOI	Law Enf Reqs	Breaches	Data Complaints	Combined
2022	285	1,195	76	275	n/a	1,831
2023	301 *(+6%)*	1,277 *(+7%)*	59 *(-22%)*	346 *(+26%)*	n/a	1,983 *(+8%)*
2024	445 *(+48%)*	1,449 *(+13%)*	100 *(+69%)*	407 *(+18%)*	n/a	2,401 *(+21%)*
2025	591 *(+33%)*	1,636 *(+13%)*	140 *(+40%)*	464 *(+14%)*	51	2,882 *(+20%)*
Projections for 2026 based on Jan – Mar figures						
2026	645 *(+9%)*	2,097 *(+28%)*	126 *(-10%)*	531 *(+14%)*	37 *(-27%)*	3,436 *(+19%)*



The vast majority of organisational change activity requires input from the team, as will more often than not either result in new technology and/or change the way that personal information is processed. This will require subject matter expert input into Data Protection Impact Assessments, as well as advising on matters such as data sharing and data privacy agreement.

The Data (Use and Access) Act introduced a mandatory internal complaints process before escalation to the ICO, which has put further pressure on the team.

Automation has been employed to ease some of the administrative burden, but caseloads continue to increase at a faster rate than any mechanisms to improve efficiency.

Key Developments 2025/26

- Automation of some aspects of the Freedom of Information process;
- Recruitment into vacant posts;
- Rollout of Data Protection Impact Assessment screening tool

Key Actions for 2026/27

- Seek extension to the Data Protection Analyst post;
- Explore use of AI agents to support Data Protection Impact Assessment process;
- Seek Service Design support to challenge existing team processes and structure

Risk:	43	Inadequate leadership and oversight of data protection activities at a strategic and operational level results in poor information compliance culture			
Low		**Risk Owner(s)**	Marc Eyre / James Fisher (Assurance – Information Compliance)	**Reviewed**	31/03/26

Current Position (including audit action status)

The Council has a Strategic Information Governance Board, supported by a number of operational working groups. The Strategic Board is chaired by the Director for Legal and Democratic (as the Senior Information Risk Owner) providing escalation to the Senior Leadership Team as appropriate, and has membership from Directorate Management Team representatives alongside information governance professionals). The Board reports to both SLT and Audit & Governance Committee annually (via this Annual Information Governance report), and more regularly where required. It monitors a range of Key Performance Indicators across the range of information governance activities, and maintains an improvement action plan mapped to the Information Commissioners accountability framework. Working groups include the Operational Information Governance Group, which is a consultee in the transformation process, and has representation on the Technical Design Authority, and the Cyber Technical Group. There are no outstanding audit requirements associated with this risk, which is managed to an acceptable level.

Key Developments 2025/26

- Development of Key Performance Indicator set

Key Actions for 2026/27

- Implement any proposed changes resulting from the Governance review.

Risk:	44	Inadequate compliance with individual rights under data protection law		
Low	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)

Individual Rights allows data subjects to enact certain powers over their personal information that is held. The most common and well known of these rights is the right of access, commonly referred to as subject access requests (SARs). This gives individuals the right to obtain a copy of their personal data held by an organisation, as set out in the General Data Protection Regulations.

The Information Compliance team manage the whole process for Childrens Services, which is often extremely sensitive and onerous (primarily care leaver requests, for an entire history of their care), requiring significant redaction. For other Directorates, the Information Compliance Team facilitate and advise, but the document discovery and redaction is managed within the Directorate.

Currently compliance levels for Subject Access Requests remain satisfactory, although target timescales cannot always be achieved for the largest most onerous requests. Where necessary we outsource larger more complex cases to an external provider.

The following chart highlights compliance rates for managing Subject Access Requests within statutory timescales (Green = ICO recommended 90% compliance; Amber = between 80-90%; Red = below 80%):

Percentage of Subject Access Requests Handled on Time

	Whole Authority		Adults & Housing		Childrens		Corporate		Place		Public Health & Prevention	
Q4 25/26												
Q3 25/26	93%	(96)	89%	(9)	96%	(71)	89%	(9)	71%	(7)		(0)
Q2 25/26	88%	(110)	83%	(12)	92%	(83)	67%	(12)	100%	(2)	100%	(1)
Q1 25/26	96%	(90)	100%	(8)	96%	(68)	91%	(11)	100%	(3)		
Q4 24/25	98%	(66)	100%	(8)	98%	(53)	100%	(2)	100%	(3)		
Q3 24/25	96%	(94)	94%	(16)	98%	(64)	60%	(5)	100%	(9)		
Q2 24/25	92%	(86)	89%	(9)	94%	(66)	67%	(6)	100%	(5)		
Q1 24/25	95%	(81)	94%	(16)	100%	(51)	73%	(11)	100%	(3)		

We have reviewed our policies and procedures in relation to release of the most sensitive information, following counsel's opinion gained following an alleged data breach. An overdue priority 2 action remains outstanding following a SWAP internal

audit report, which referenced applying the good practice adopted for Childrens SARs to other services. It was originally intended to review this as part of Our Future Council restructuring, but the Information Compliance function after review were not included within the year one considerations. This audit action will be explored further now that the Business Support hub is operational.

Key Developments 2025/26

- Improved processes, following Counsels opinion

Key Actions for 2026/27

- Explore options for replicating good practice from Childrens SARs with Business Support Hub

Risk:	45	Insufficient transparency around Dorset Council's data processing activities			
Medium		**Risk Owner(s)**	Marc Eyre / James Fisher (Assurance – Information Compliance)	**Reviewed**	31/03/26

Current Position (including audit action status)

The Information Governance action plan includes two specific actions relating to this risk:

i) for Information Asset Owners to review their schedule of privacy notices; and

ii) ii) incorporating privacy information into data protection training.

These both have a Priority 4 (low) ranking.

Key Developments 2025/26

- None

Key Actions for 2026/27

- Privacy notice review to continue, alongside services' development of information asset records.

Risk:	47	Contracts and data sharing arrangements do not comply with statutory data protection standards		
Medium	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)
A new Data Sharing policy was approved at September 2024 Strategic Information Governance Board. A log of Data Sharing Agreements has been initiated, by integrating into the roll out of the Information Asset Register. Standard data protection clauses are contained within contracts.
Key Developments 2025/26
• None
Key Actions for 2026/27
• Data sharing agreements to continue to be logged, alongside services' development of information asset records.

Risk:	48	Failure to complete data protection impact assessments prior to commencing or changing high risk data processing activities		
Medium	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)

The Data Protection Impact Assessment (DPIA) process is used to identify, assess, and reduce the privacy risks of a project, policy or change to process that involves handling personal data. DPIAs support organisations in understanding how data processing might affect individuals' rights, evaluates whether the planned activities comply with data protection laws like GDPR, and documents the steps taken to minimise risks. DPIAs are a statutory requirement for any high risk data processing and are a proactive check to ensure that any new system, technology, or process that uses personal data is designed to be safe, lawful, and respectful of people's privacy.

All high risk DPIAs are presented to the Operational Information Governance Group and signed off by the chair. To support services, a new DPIA screening tool has been developed and currently in the process of rollout. There remains a concern that not all higher risk data processing changes are undergoing DPIA either at an appropriate stage in the project lifecycle or at all. Further work is underway to embed DPIA within the transformation process.

Key Developments 2025/26

- Development of DPIA screening tool;
- Assessment and approval of DPIAs via Operational Information Governance Group

Key Actions for 2026/27

- Reporting of DPIAs via Strategic Information Governance Board;
- Explore opportunity to develop an AI agent to support services' writing DPIAs.

Risk:	49	Failure to detect, investigate, risk assess, record and respond to data breaches		
Medium	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)

A data breach can be classed as any incident where personal data is incorrectly accessed, disclosed, amended, destroyed or lost. If the breach is likely to result in a risk to the rights and freedoms of individuals, the incident must be reported to the Information Commissioner's Office (ICO), who will consider the incident, including the adequacy of the council's response. In response, the ICO may make recommendations to the council aimed at mitigating the breach or preventing further occurrences. In the most serious cases, the ICO may take enforcement action against the council, including issuing a monetary penalty. Where the ICO have historically taken enforcement action against local authorities, they have on occasion levied significant 6-figure sums for personal data breaches, and in the most serious cases they have power to fine a local authority up to £17.5 million.

The chart below summaries the cause of data breaches received over the last two years:

Row Labels	**2024**	**2025**
Unauthorised disclosure by email	290	317
Unauthorised Internal Access	16	16
Information Lost	14	15
Unauthorised Online Publication	21	32
Unauthorised disclosure by post	23	29
Unauthorised disclosure by telephone	9	11
Failure to redact	n/a	9
Other	34	35
Grand Total	**407**	**464**

Of the 464 cases, 17 were determined necessary to refer to the Information Commissioner. None have resulted in any regulatory action.

The majority of losses across both years relate to email disclosures. In response, the capability within the Microsoft E5 licencing on Data Loss Prevention and Email encryption has been enabled, linked to an improved application of sensitivity labels. Data Loss Prevention is a capability within Microsoft Purview that includes prompts to users where certain risk data is included within an email, to reduce the risk of information being incorrectly shared, and in certain cases restricts sending where the incorrect labelling is applied. This is an ongoing piece of work, which continues to

strengthen the management of emails. Whilst on one hand it reduces the risk of data breach, it is worth emphasising that it equally raises awareness that a breach has occurred, which means that we can expect a temporary increase in reporting.

SWAP undertook an internal audit of Dorset Council's rollout of Purview in Q4 of 2025/26. It recognised that the Council's approach is both proactive and at the forefront of local authority data loss prevention methods. Actions were identified however in terms of mapping future rollout to the Council's risk appetite, to support prioritisation and resourcing. This will be the subject of discussion at April's Strategic Information Governance Board.

The data breach reporting process has been improved, with reporting including an assessment of the risk that defines the level of investigation that is necessary, and enables better self service of some of the investigation process and identification of remedial actions.

Key Developments 2025/26

- Improved data breach reporting process, with automation and greater level of self service within Directorates;
- Improvements to sensitivity labelling, reducing data breach risk and enabling improved ability to recall messages

Key Actions for 2026/27

- Define strategy for ongoing Purview rollout, and appetite for use of insider risk management tools to identify potential data breach risks and employing default labelling for services, based on risk.

Risk:	50	The Council does not adhere to the Information Commissioner's Code of Practice in relation to the Freedom of Information and Environmental Regulations requests, resulting in regulatory enforcement and reputational damage		
Low	**Risk Owner(s)**	Marc Eyre / James Fisher (Assurance – Information Compliance)	**Reviewed**	31/03/26

Current Position (including audit action status)

The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) gives a general right of access to information held by public authorities. The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. Compliance rates are shown below:

Percentage of FOI Requests Handled on Time

	Whole Authority		Adults & Housing		Childrens		Corporate		Place		Public Health & Prevention	
Feb-26	83%	(132)	65%	(17)	71%	(17)	90%	(41)	86%	(42)	87%	(15)
Jan-26	86%	(125)	64%	(14)	69%	(13)	91%	(35)	94%	(49)	79%	(14)
Dec-25	85%	(150)	68%	(22)	91%	(22)	91%	(44)	83%	(46)	94%	(16)
Nov-25	86%	(147)	56%	(9)	86%	(22)	87%	(53)	92%	(48)	87%	(15)
Oct-25	89%	(131)	75%	(12)	80%	(15)	92%	(38)	89%	(54)	100%	(12)
Sep-25	86%	(137)	79%	(14)	63%	(16)	92%	(37)	87%	(55)	100%	(15)
Aug-25	92%	(145)	85%	(13)	94%	(18)	93%	(44)	93%	(59)	91%	(11)
Jul-25	86%	(130)	58%	(12)	58%	(12)	95%	(39)	92%	(53)	86%	(14)
Jun-25	80%	(140)	55%	(22)	50%	(10)	87%	(47)	89%	(47)	86%	(14)
May-25	83%	(123)	62%	(13)	83%	(12)	72%	(36)	92%	(51)	100%	(11)
Apr-25	84%	(140)	78%	(23)	67%	(18)	80%	(44)	96%	(48)	100%	(7)
Mar-25	86%	(129)	60%	(10)	86%	(22)	88%	(41)	89%	(56)		
Feb-25	88%	(139)	67%	(15)	91%	(22)	90%	(40)	90%	(62)		
Jan-25	91%	(106)	90%	(20)	92%	(13)	92%	(26)	89%	(47)		
Dec-24	83%	(127)	60%	(15)	71%	(14)	84%	(51)	91%	(47)		
Nov-24	87%	(132)	86%	(21)	69%	(13)	98%	(40)	84%	(58)		
Oct-24	88%	(115)	79%	(19)	73%	(15)	90%	(42)	95%	(39)		
Sep-24	87%	(98)	73%	(11)	75%	(12)	93%	(28)	89%	(47)		
Aug-24	86%	(119)	70%	(20)	70%	(23)	97%	(37)	92%	(39)		
Jul-24	84%	(106)	91%	(11)	63%	(8)	84%	(43)	86%	(44)		
Jun-24	81%	(112)	55%	(11)	65%	(20)	84%	(44)	95%	(37)		
May-24	85%	(126)	94%	(16)	67%	(15)	87%	(39)	86%	(56)		
Apr-24	90%	(136)	79%	(14)	80%	(10)	98%	(45)	90%	(67)		
Mar-24	81%	(109)	64%	(11)	74%	(19)	81%	(43)	89%	(36)		

Whilst this remains a low risk managed to an acceptable level, this is challenged by a significant increase in both the number and complexity of information requests (with artificial intelligence supporting users in submitting detailed requests, increasing the level of disclosure required).

Key Developments 2025/26

- Maintaining positive compliance rates, despite significant increase in caseloads

Key Actions for 2026/27

- Seek Service Design support to challenge existing team processes and structure;
- Ongoing development of publication scheme, and supporting services with improved transparency of documents.

Risk:	52	Data loss / leakage by internal staff / leavers		
Medium	Risk Owner(s)	Marc Eyre / James Fisher (Assurance – Information Compliance)	Reviewed	31/03/26

Current Position (including audit action status)

Employees who have access to the highest levels of classified data are in an advantageous position to commit data thefts, presenting a need for employer diligence and monitoring. We have in place identity access management systems, restrict access to data outside of networks, monitor employees for high-risk or anomalous behaviour, and review security protocols regularly.

There are clear guidelines on manager responsibilities for staff leaving employment, which includes ensuring sensitive information is returned or destroyed. We have had two incidents where it is believed agency workers have left the employment and withheld sensitive information. It should be noted however that some additional controls have been implemented by the Directorate.

The MS Purview product includes Insider Risk Management capability which provides a number of tools to prevent the risk of data loss. This includes highlighting data transferred to external devices and any significant data transfer once an employee has handed in notice. If supported for roll-out and resourcing by Strategic Information Governance Board, this will help highlight where this risk may be likely to occur.

An Account Activity Policy was supported for adoption by the Operational Information Governance Group in December 2024, but there remains a need to look at issues with the Starters, Leavers and Movers process.

Key Developments 2025/26

- Ongoing rollout out of MS Purview tools

Key Actions for 2026/27

- Define strategy for ongoing Purview rollout, and appetite for use of insider risk management tools to identify potential data breach risks.

Risk:	55	Failure to comply with Regulation of Investigatory Powers Act 2000 or other covert surveillance legislation			
Medium		**Risk Owner(s)**	Marc Eyre / James Fisher (Assurance – Information Compliance)	**Reviewed**	31/03/26

Current Position (including audit action status)

The Council operates a "Use of Covert Surveillance" policy to meet the requirements of Regulation of Investigatory Power Act (RIPA) and associated surveillance legislation, including occasions where covert surveillance is necessary, but not meeting the RIPA threshold. The policy sets out that the Audit and Committee will be informed annually on the following covert surveillance activity:

- The number of RIPA authorisations requested and granted – One underway during 2025/26;
- The number of RIPA light authorisations requested and granted – One during 2025/26;
- The number of times social networking sites have been viewed in an investigatory capacity - No RIPA authorisations or RIPA light authorisations were requested or granted for surveillance of social networking sites

There are no outstanding audit actions.

Key Developments 2025/26

- None

Key Actions for 2026/27

- There is an outstanding action in the Information Governance action plan to roll out training for approving officers.

Risk:	117	As a result of inaccurate business intelligence, uninformed decision making may take place at a strategic level leading to a failure to deliver the Council's services and/or priorities effectively			
Medium		**Risk Owner(s)**	Chris Heighway / Chris Swain / Michael O'Donovan (Strategy) / Liz Crocker	**Reviewed**	31/03/26

Current Position (including audit action status)

In accordance with the Council's Strategic Performance Management Framework, business intelligence represents the collation and integration of a wide range of data, including financial management information, operational performance, Council Plan delivery, risk management, audit actions, national benchmarking, resident and workforce satisfaction, and wider horizon-scanning intelligence. Because data sources vary from internal systems to national datasets, data quality and validation are critical controls in mitigating the risk of inaccurate intelligence informing strategic decisions.

All employees involved in inputting performance data and accompany performance narrative are accountable for ensuring its quality, accuracy and integrity. This includes adherence to GDPR requirements and ensuring that data is fit for purpose before it enters strategic reporting channels.

For strategic performance monitoring, the Performance Indicator Library plays a key role in ensuring consistency and clarity. It includes clear up-to-date definitions, an audit trail of changes, named data owners, and details of data sources and collection methodologies — strengthening transparency and supporting accurate interpretation.

Strategic performance and risk information is reported quarterly to SLT, Informal Cabinet and Scrutiny Committees, with information flowing through the performance framework from operational teams to Directorate Leadership Teams before reaching corporate oversight. These internal checkpoints ensure that service leads remain accountable for their data and metrics, helping to reduce the likelihood of incomplete or inaccurate intelligence reaching strategic decision-makers.

Data presented to senior leaders has strengthened in recent quarters, including enhanced Council Plan reporting and supplementary updates that track improvement actions. This has improved both transparency and assurance across the organisation.

The strategic risk register and wider risk governance arrangements are also reported quarterly to Audit & Governance Committee, providing an additional assurance mechanism over the control environment and the quality of supporting intelligence.

The Policy Intelligence and Performance Service have also developed reporting dashboards to ensure access to well-presented data. This supports informed decision making and reduces the reliance on manual interpretation.

Key Developments 2025/26

During 2025/26, significant work has been undertaken to improve the quality and integration of performance, risk and business intelligence. Key developments include:

- Published the Strategic Performance Management Framework, clarifying expectations for performance reporting.
- Developed the Performance Indicator Library to standardise definitions and strengthen data quality.
- Introduced Council Plan monitoring and dashboards to improve visibility of delivery.
- Completed the annual review of performance and risk indicators with service leads.
- Updated and enhanced the dashboard portfolio to improve insight and usability.
- Updated the strategic risk register alongside the new audit and audit-actions register.
- Strengthened collaboration between the strategic hub and embedded business intelligence and performance teams in directorates to improve data quality and insight.

Key Actions for 2026/27

- Develop an improved interface for performance data input and narrative, creating a stronger underlying data structure that supports future automation and integration with evolving data architecture.
- Incorporate benchmarking analysis into the dashboard portfolio, including metrics from the new national Local Outcomes Framework and LG Inform+.
- Continue embedding a strong culture of performance reporting and data quality through targeted internal communications, training and support for directorate teams.

Risk:	326	Because information management policies are not consistently applied, controls over how information is stored and maintained may not be followed, resulting in unnecessary data growth, duplication, security vulnerabilities and increased operational costs		
Medium	**Risk Owner(s)**	Sam Johnston / Kate Watson (Archives and Information Management)	**Reviewed**	17/12/26

Current Position (including audit action status)

Under the Information Asset Ownership (IAO) model, responsibility for the effective management of information sits with services. Service managers and Heads of Service, acting as Information Asset Owners, are accountable for decisions relating to their information assets, including how information is stored, reviewed and disposed of, and for managing the associated risks within their areas. This role supports the Senior Information Risk Owner (SIRO) by providing assurance at service level.

The Information Governance policy requires Information Asset Owners to understand what information they hold, assess whether it remains necessary, and ensure information is disposed of in line with the Council's retention schedules or transferred to the Dorset History Centre where appropriate.

To support services in meeting these responsibilities, the Records Management team have developed training modules and guidance to help Information Asset Owners manage information assets and maintain accurate records within the Information Asset Register and Register of Processing Activities (IAR and ROPA), as required under the UK General Data Protection Regulation. These arrangements operate on a self-service basis, with services expected to identify, review and maintain their own information assets.

However, application of these controls is currently inconsistent across the organisation. Completion of training and the population and ongoing review of the IAR and ROPA remain low, limiting the Council's ability to demonstrate consistent oversight of information assets and increasing the risk of unnecessary data retention, duplication and unmanaged information.

The SWAP Data Maturity Audit identified actions to strengthen assurance in this area, including the development of Key Performance Indicators (KPIs) to monitor compliance with information management requirements. These measures will support more consistent reporting and enable senior officers, through the Strategic Information Governance Board, to take targeted action where controls are not being effectively applied.

Key Developments 2025/26

- Information Asset Owner (IAO) training pathway for managers made available, including a practical checklist setting out the typical activities expected of the role
- Quarterly notifications are sent to IAOs highlighting overdue decisions relating to paper records, supported by intranet guidance on using the self-service records management system
- Information Asset Owner guidance was included in knowledge transfer intranet pages, to support the effective handover of information when staff leave the organisation or move roles.

Key Actions for 2026/27

- Key Performance Indicators (KPIs) will be finalised and published, covering training completion, Information Asset Register and Record of Processing Activities entries, and timely paper records disposal decisions
- The dashboard will be made available on the performance area of the intranet
- Further targeted communications will be issued to Information Asset Owners
- The Strategic Information Governance Board meeting in April will consider options to strengthen assurance by making Information Asset Owner training mandatory for relevant roles
- The effectiveness of existing self-service approaches, including training materials and guidance will be regularly reviewed.

6. Alternative options considered

6.1 N/A

7. Legal considerations

7.1 Ensure that the Council is meeting the obligations of the forthcoming “Data (Use and Access)” Bill, alongside the UK General Data Protection Regulation.

8. Financial implications

8.1 There are no direct financial implications from this report. However, the General Data Protection Regulation sets out that the Data Protection Officer must be provided with sufficient resources to perform their role. The ongoing work of the Strategic Information Governance Board may identify areas where additional resourcing is required.

9. Natural environment, climate & ecology implications

9.1 Good quality and managed data is essential in supporting our climate change agenda

10. Well-being and health implications

10.1 Good quality and managed data is essential in supporting health and wellbeing

11. Other implications

11.1 None

12. Risk implications

12.1 HAVING CONSIDERED: the risks associated with this decision; the level of risk has been identified as:

Current Risk: High

Residual Risk:High

This scoring reflect that there are a number of High and Very High strategic and operational risks referenced within this report.

13. Equalities

13.1 None

14. Appendices

14.1 None

15. Background papers

15.1 None

16. Report sign-off

15.1 This report has been through the internal report clearance process and has been signed off by the Director for Legal and Democratic (Monitoring Officer), the Executive Director for Corporate Development (Section 151 Officer) and the appropriate Portfolio Holder(s)