Audit and Governance Committee

4 August 2025

Annual Information Governance Report – 2024/25

For Review and Consultation

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

Local Councillor(s): N/A

Executive Director:
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:

Report status: Public Choose an item.

1. Executive summary

1.1 This is the third Annual Information Governance Report, to be presented to both Senior Leadership Team and 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 Appendix A to this report sets out background information on the Council's information governance structures. This should provide some context to new members of the committee.

1.3 Key Developments in 2024/25 included:

- **Policy Updates**: New policies were introduced for Use of AI and data sharing, while existing ones like records management were refreshed. Email encryption and Data Loss Prevention tools were implemented to reduce data breach risks.
- **AI Governance**: Microsoft Co-Pilot was approved for internal AI needs, while third-party AI tools were blacklisted unless demonstrated by a clear business need.

- **Cyber Security and ICT Continuity**: Cyber threats remain a “very high” risk. Investments were made in Microsoft E5 capabilities and cyber monitoring. Training and phishing simulations are conducted. A successful ICT continuity exercise during Easter reduced the strategic risk level for ICT continuity.
- **Records Management**: A simplification project was launched to migrate content from shared drives to Microsoft 365. Training for Information Asset Owners was delivered, and improvements were made to paper records tracking.
- **Subject Access Requests (SARs)**: SARs rose by 39% to 478, with 78% related to Children’s Services. Despite the increase, compliance exceeded 90% in all quarters due to improved processes and team integration.
- **Freedom of Information (FOI)**: 1,445 FOI/EIR requests were received. While the 90% response target was met in only two months, compliance stayed above 80% throughout the year. Transparency initiatives are underway to manage rising volumes.
- **Data Breaches**: 382 breaches were reported (up from 376), with 14 reported to the Information Commissioner. Email misuse accounted for 71% of incidents. No enforcement actions were taken. New sensitivity labels and breach monitoring tools were introduced.
- **Training Compliance**: Data protection training compliance ranged from 80–89%, below the 95% target. Cyber training compliance dropped to 65%. Senior Leadership Team have approved introducing system access restrictions for non-compliance.

1.4 Looking Ahead to 2025/26, priorities include:

- Developing a Power BI policy
- Ongoing roll out of the Information Asset Register
- Enhancing breach response mechanisms
- Enabling improved compliance on information governance training
- Supporting the “Our Future Council” transformation programme

1.5 The upcoming Data (Use and Access) Bill introduces a mandatory internal complaints process before escalation to the ICO. Dorset is preparing by establishing a dedicated complaints database, which will be supported by a policy document.

2. Recommendation(s)

2.1 To note the 2024/25 activity and focus for 2025/26.

3. Reason for the recommendation(s)

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

4. Information Governance Activity During 2024/25

4.1 A number of policies have been updated via the Operational Information Governance Group (OIGG) and signed off by the Strategic Information Governance Board (SIGB) during 2024/25:
- Use of AI Automation Algorithmic Data Processing (New policy)
- Data Sharing (New policy)
- Records Management (Refresh)
- Acceptable Use (Refresh)
- Business Continuity Framework (Refresh)

4.2 Data Loss Prevention and Email encryption have been enabled, both linked to the use 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. Additional controls have also been implemented to assist the identification of out of date membership of shared inboxes (for instance where staff move roles internally), to ensure that data isn't unnecessarily shared.

4.3 The OIGG has received, challenged and approved 12 Data Protection Impact Assessments (DPIA) during 2024/25. This has included:

- AI Communications Mining tool;
- Booking Solutions;
- Care Dorset
- Citizens Space
- Digitisation of Mental Health Act Assessments;
- Drug related deaths;
- E-signatures;
- Parent Assess;
- Right Care at Home;
- Sharing of Equality Data;
- Urgent and Emergency Care Transformation;
- Use of Microsoft Co-pilot;
- Whole Family Working

4.4 An improved workflow for DPIAs is in development. It is recognised that the Our Future Council programme will be looking to deliver efficiency through technology use. This will impact on the work programme for the OIGG, as it is anticipated that there will be a significant increase in DPIAs.

4.5 The OIGG is linked in closely with the developing AI agenda, in line with the Use of AI, Automation and Algorithmic Data Processing policy. An assessment was undertaken of the number of different AI tools that have been accessed by staff. There are risks associated with this use, particularly where sensitive information is included, and without appropriate governance sensitive information could be retained and incorporated into the AI tools models. The decision was taken to blacklist the use of third party AI tools, as the functionality is provided by Microsoft Co-Pilot. As a Microsoft customer, the use of this application ensures that our data remains within our domain. There is a process to whitelist where there is an identified business need. An Acceptable Use of AI policy has recently been approved.

4.6 **Cyber Security**

4.6.1 During 2024/25 a number of local authorities suffered high profile attacks and/or continue to recover from the consequences of the incident. Because of this inherent risk, the threat of a successful cyber attack is currently identified as a "very high" risk in the Council's risk register.

4.6.2 Cyber security has made steady progress over the last year. The council is working to build on Microsoft E5 licence baseline capabilities to increase the organisation's ability to detect and respond to threats within our infrastructure. The intention is to invest further in employing a small team of cyber risk specialists, to significantly improve our ability to use the cyber monitoring data to identify actions to strengthen our technical defences. Third party monitoring would also be funded by these additional funds to provide a managed service providing out of hours monitoring service and response to cyber threats. This is subject to consideration as part of transformation proposals.

4.6.3 Cyber security training is mandatory for all officers and councillors, and is delivered via small bitesize modules to ensure that the content remains relevant to the most current threats. Performance is covered within 3.5 of this report. Training is supported by phishing simulations to test the extent of understanding.

4.6.4 Over the Easter Bank Holiday period, an ICT service continuity exercise was undertaken, to co-incide with planned maintenance. This provided positive assurance, to the extent that the strategic risk relating to ICT service continuity has reduced from "very high" to "high". By very nature of the

consequences, the inherent risk will always remain at quite a high level. There were a number of lessons learnt, and an action plan is in development.

4.6.5 Directorates are reviewing their Business Impact Assessments and supporting business continuity action cards, which include resilience against the cyber risk. A set of business continuity exercises are available to services, to allow them to test their current resilience to both cyber attack and any resultant loss of data. This initiative was recognised by ALARM – the Public Sector Risk Management Association, who shortlisted it as a finalist within their annual awards, under the "resilience" category.

4.7 The Council's Data and Business Intelligence Strategy which was approved in February 2023 will be superseded by a Data and Technology Strategy later this year. This will include a focus on automating key processes to safeguard data quality, improve the self-service offerings, and address pain points in the customer experience.

4.8 **Information Management**

4.8.1 The Records Management Policy has been refreshed to more clearly define the role of Information Asset Owners in managing the risks to their service's information.

4.8.2 Work on the Simplifying Records Management workstream has resulted in a proposal focusing on migrating necessary content from shared drives and improving use of Microsoft 365. This is an important foundation for Our Future Council, supporting services to work efficiently with their information organised and in one place. Internal funding was sought from Senior Leadership Team for this business case, but it was not supported. However there remains a commitment for services to deliver migration within existing resources. An updated plan will be presented to SLT in October 2025.

4.8.3 An introductory training session was provided for all Information Asset Owners in February 2025, covering the responsibilities of their role and some of the tools available to them. Self-directed learning content is now being developed to assist managers with contributing to the Information Asset Register.

4.8.4 New Sensitivity labels for emails and Microsoft Office tools, and supporting information handling guidance, have been made available to all employees. Site container labels have also been updated - both informed by Government good practice.

4.8.5 Improvements have been made to the in-house system for tracking paper files held at the Records Management Unit. These changes will enable Information Asset Owners to manage their paper files more easily, and customers to track progress of their paper records transfers.

4.8.6 A new 2-year project has started to improve the management of paper and digital children's records. This will involve increasing the retention period for all records belonging to care-experienced and adopted children, restarting file disposals after a long-term nationwide hold, consolidating paper records into one storage location and supporting Children's Services managers to contribute to the Information Asset Register.

4.9 All organisations that have access to NHS patient data and systems must annually complete the NHS Data Security and Protection toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. A failure to meet the requirements of the toolkit could compromise the Council's ability to access NHS data, which is pivotal to service delivery. The toolkit was completed in June 2025, but recognised that the Council was still not meeting the mandatory requirements on data protection and cyber security training. As a result, the Council remains subject to an action plan to improve compliance rates on mandatory training. The risks associated with non-compliance with the toolkit are equally applicable to the Public Services Network and other ICT assurance frameworks.

4.10 The Council operates a "Use of Covert Surveillance" policy to meet the requirements of Regulation of Investigatory Power Act (RIPA) and associated surveillance legislation. This extended the policy to include those 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 – None during 2024/25;
- The number of RIPA light authorisations requested and granted – None during 2024/25;
- 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

5. Performance and Risk

5.1 A range of performance indicators are monitored in respect of the Council's information compliance arrangements. These are not replicated in full here, but top level "whole Council" figures have been included.

5.2 **Public and Environmental Information Requests**

5.2.1 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. During 2024/25, the Council received 1,445 requests (approx. 120 per month).

5.2.2 The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. Whilst this was met in only two months during 2024/25, compliance exceeded 85% in nine of the twelve months, and at no point dropped below 80%. With Freedom of Information request numbers on the increase (6% from 2023/24), there is pressure on both the Information Compliance Team and responding services. As part of effort to manage this increase, the Council implemented a degree of automation, to carry out the reminder element of the process. It had been hoped to provide further automation, but this was restricted as there is insufficient data from request numbers to train an AI model. Work is underway to understand the most regular requests and determine if more can be done with signposting and information transparency to reduce requests. The Information Commissioner's Publication Scheme, which sets out documents that authorities should look to publish, has also been reviewed, and the Information Compliance team are liaising with services where there are gaps.

	Whole Authority	**Adults & Housing**	**Childrens**	**Corporate**	**Place**
Mar 25	86% (129)	60% (10)	86% (22)	88% (41)	89% (56)
Feb 25	88% (140)	67% (15)	91% (22)	90% (40)	90% (62)
Jan 25	91% (107)	90% (20)	92% (13)	96% (25)	88% (48)
Dec 24	83% (128)	64% (14)	67% (15)	84% (51)	91% (47)
Nov 24	87% (133)	86% (21)	69% (13)	98% (40)	84% (58)
Oct 24	88% (116)	79% (19)	73% (15)	91% (42)	95% (39)
Sep 24	87% (99)	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	82% (114)	55% (11)	65% (20)	84% (44)	95% (37)
May 24	85% (127)	94% (16)	67% (15)	87% (39)	86% (56)
Apr 24	91% (137)	79% (14)	80% (10)	98% (45)	90% (67)

5.2.3 For clarification, Corporate includes the following services: Legal; Democratic and Elections; Assurance; Finance; ICT; Human Resources; Strategy Performance and Sustainability; Transformation Customer and Cultural Services.

5.2.4 Place includes the following: Highways; Waste; Planning; Transport; Assets and Regeneration; Community and Public Protection; Environment and Wellbeing.

5.2.5 The following chart shows the number of FOIs overdue by more than 20 days (ie over 40 days from receipt). We have started to collect this information with effect from December 2024, and what it demonstrates is that even where we are not meeting the 90% target, it is rare for FOIs to exceed the target by much:

	Whole Authority	**Adults & Housing**	**Childrens**	**Corporate**	**Place**
Mar 25	3	3	0	0	0
Feb 25	3	2	1	0	0
Jan 25	3	3	0	0	0
Dec 24	1	1	0	0	0

5.2.6 Within Adults and Housing there is a process established for Corporate Director sign off to provide assurance over the information being released. This has caused some delay, rather than the collection of data which is generally collected within timescale. FOIs are becoming more complex in their ask for information, which can impact on the timeliness of the information as it is often a response requiring input from a number of officers.

5.3 **Requests Relating to Personal Information**

5.3.1 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 or 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. During 2024/25 the Council received 478 SARs, up from 343 in the previous financial year. Of these, 317 became active (up from 266), approx. 27 per month (up from 22). Of these, 78% related to Childrens Services (up from 63%). Children's Services requests (and in particular those requested by care leavers) involve highly sensitive and significant case files that require careful review and redaction.

5.3.2 Since GDPR legislation became law in 2018, requests had increased at a rate of approximately 24% year on year, although this trend appeared to plateau in the 2023/24 financial year. This year, there has been an increase of 39% on requests and 19% on active requests.

5.3.3 Historically the Council has struggled to meet compliance with statutory timescales, with regularly reporting as a “Red” performance indicator (below 80% compliance). Significant progress has been made to improve performance since the SARs team were integrated into the Information Compliance team (tasked with completing all Children’s Services requests) in early 2022. Compliance was above the 90% target set by the Information Commissioner in all four quarters, which is a significant achievement, given the increased number of requests and their complexity.

5.3.4 The improvement in performance has been achieved through an effective and efficient two stage review process, and dedicated professional knowledge within the SAR team enhanced by training. The need reported in the last two years to outsource requests above capacity has been significantly reduced, but will continue to be utilised where demand exceeds capacity.

	Whole Authority	**Adults & Housing**	**Childrens**	**Corporate**	**Place**
Q4	98% (66)	100% (8)	98% (53)	100% (2)	100% (3)
Q3	95% (84)	83% (6)	98% (64)	60% (5)	100% (9)
Q2	92% (86)	89% (9)	94% (66)	77% (6)	100% (5)
Q1	95% (81)	94% (16)	100% (51)	73% (11)	100% (3)

5.3.5 The chart above highlights red performance within corporate services. It should be noted that request numbers are low. Equally the compiling, reviewing and redaction will be undertaken by the service holding the information, rather than the corporate team (who manage the whole process for Childrens requests), and therefore not benefitting from the dedicated knowledge and skillsets that that central team provides.

5.3.6 Outside of the 2024/25 timescales within scope for this report, there has been a significant data breach relating to the SARs process and sensitive childrens services data. This prompted the Service Manager for Assurance to initiate an internal audit on the SARs process, in addition to personally carrying out a review of the incident. Whilst the breach was regrettable, and a matter of human error, the committee can be assured that the internal audit process has presented a reasonable level of assurance. The auditor acknowledged

that the childrens services SARs process alone would have presented a substantial assurance, and there is some good practice that could be extended to other directorate requests.

5.4 **Data Breaches**

5.4.1 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.

5.4.2 The 2024/25 financial year saw an increase in the number of breaches internally reported by council services. There were 295 incidents reported in 2022, which increased to 376 in 2023. This has continued an upward trajectory to 382 breaches reported for 2024/25. 14 of these incidents were determined by the Data Protection Officer to meet the criteria for escalation to the ICO. A further 2 were reported to the ICO by an external individual or organisation. There has been no enforcement action by the ICO, but on several occasions recommendations have been made and actions mandated. The causes of data breaches during 2024/25 are summarised below:

Incident Category	**Frequency in 2024/25**	**% of recorded incidents**
Email	271	71%
Fax	1	0%
Post	20	5%
Unauthorised online access	33	9%
Unauthorised internal access	19	5%
Lost	11	3%
Telephone	10	3%
Other (including AI bots)	17	4%

5.4.3 As can be seen from the figures above, 71% of breaches relate to the use of email. Email security is already a core part of the council's mandatory data protection and cyber security training for all staff. As reported earlier in the report, technology is being used to help reduce the data breach risk, through improved email encryption and use of Data Loss Prevention tools. Similarly the introduction of sensitivity labelling provides the ability to revoke access. These mechanisms are in their infancy, and further work is underway to embed and enhance, and will be monitored. Over time it is hoped that this will reduce breaches, but there is acceptance that in the short term we may see an increase due to a higher awareness of what constitutes a breach and needs reporting (as it is likely there is currently under reporting).

5.4.4 Where a data breach has occurred appropriate management action is considered on a case-by-case basis, dependent upon the severity of the breach and level of culpability. In the last year formal action has been taken in several cases.

5.4.5 The Organisational Compliance and Risk Learning Group has been operating since the beginning of 2023/24. The role of this includes cross-Directorate challenge to the more serious breaches, to ensure that appropriate whole council learning can be identified and improved control mechanisms established. This group aims to review all data breach incidents that are reported to the ICO. Change of officers has impacted on this group meeting over the last six months, and it is recognised that this group is a key function of the Council's information governance arrangements.

5.5 **Mandatory Data Protection and Cyber Training**

5.5.1 Officers and members are required to undertake mandatory training for both data protection and cyber. Both are delivered primarily via e-learning, with data protection training completed annually, whereas cyber security training is delivered in bite-size chunks. Training on both areas is also incorporated into the elected member induction programme.

5.5.2 The mandatory data protection compliance training remains stubbornly between 80% and 89% across the last six months, but is still short of the target 95%. At the time of writing this report cyber training compliance is at approximately 65%, which has reduced from the 73% reported last year. As highlighted earlier in the report, this presents a continuing risk to compliance with the NHS Data Security and Protection toolkit.

5.5.3 There remain regular reminders, and managers have access to dashboards to identify where staff are not completing either training module. The Operational Information Governance Group has supported introducing removal of systems access to those that have not carried out the training within a reasonable period of time. This was supported by the Senior

Leadership Team in June 2025, and work is now underway to determine how this can be enabled. Where the removal of access to IT systems can directly impact on an employee's ability to undertake their role, appropriate management action can be taken.

5.6 The Council's risk register identifies 42 risks in the Data and Information Management risk category, five of which are identified as "High" or "Very High" as set out in the table below:

Risk	Risk Ranking	Management Response	Risk Owner
107 - Inadequate evidence base (including Partnership data) to determine service need for children's care and protection	High	We have undertaken significant work to further strengthen practice and services through our Strengthening Services for Children and Families Programme. The developments in Business Intelligence are supporting us to understand and model service need and we continue to develop this approach.	Corporate Director – Care and Protection
286 - A successful cyber-attack to IT systems causes loss of service or data	Very High	By very nature, the impacts of cyber risk will always remain high and, despite the significant controls in place, remains possible. A number of local authorities have experienced cyber attacks that have had a severe impact on service delivery. The council's identity management (multifactor, conditional access and account permission) has been reviewed with the support of specialist technology. Baseline Microsoft licence E5 capabilities have been implemented.	Head of ICT Operations

Risk	Risk Ranking	Management Response	Risk Owner
		Continuous monitoring and improvement of over 60 individual elements of cyber security through increased controls. All areas are either planned, investigated or implemented to continuously improve the Councils cyber security posture.	
348 - There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure.	High	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. 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.	Head of ICT Operations
612 - Loss of the ability to find, open, work with, understand or trust Dorset Council's digital information causes disruption to	High	The Simplifying workstream is designing how to implement better protections and retention on digital information stored in Microsoft 365 and our legacy information on shared drives – ensuring it is managed through its lifecycle from creation to disposal or transfer to Dorset History Centre. This work plans to review 'orphaned' information and propose ownership by the most relevant Information Asset Owner.	Service Manager for Archives and Records

Risk	Risk Ranking	Management Response	Risk Owner
business operations		Records management requirements are now included in general requirements used when procuring new ICT systems. There is still much to be done in upgrading the retention capabilities of current line-of-business systems (e.g. Mosaic, ModGov) and putting in place differentiated controls according to the value and longevity of the information concerned. Simplifying has now reached a point where it will be shortly presented to senior officers for consideration and potential funding. A business case is due to go before the Design Authority in April 2025. If agreed, this project will address the question of the shared drives and the 94 million documents stored there - prior to switchoff in 2027 and migration of selected content to Sharepoint.	
809 - Contraction of the ICT function to contribute to meeting financial pressures results in insufficient ICT capacity and capabilities to deliver the	High	Proactively engaging in benchmarking activity with SWAP to benchmark resourcing of ICT functions across councils. Proactively engaging in the Our Future Council programme Strategic & Enabling workstream to make the case for change to the ICT establishment as part of forming the wider new 'strategic core' of the council, balancing financial pressures with the need to adopt new technologies, and deploy technologies more widely to support new ways of working	Head of ICT Operations

Risk	Risk Ranking	Management Response	Risk Owner
technology platforms that enable future ways of working and whole-council performance			

6. Focus for 2025/26 – The ICO Accountability Framework

6.1 The Government has proposed reform changes to the existing data protection legislation with the "Data (Use and Access)" Bill. The key focus is around reducing barriers to responsible innovation and mitigating the burdens on organisations whilst continuing to improve outcomes for people. These changes are not envisaged to significantly reduce impacts on public sector organisations, who by very nature of their statutory functions would be deemed to be carrying out high risk processing of personal data. One change worth highlighting however is the introduction of a data protection complaints process.

6.2 Whereas historically individuals could complain directly to the Information Commissioner, the Bill proposes that they must first submit complaints directly to the organisation. They would then be escalated to the Information Commissioner if not handled properly by the organisation (which in many ways mirrors the complaints escalation route via the ombudsman). The aim of this is to give organisations the opportunity to resolve issues without escalation, and ensure that the Information Commissioner's capacity is focussed on the most significant complaints. The Information Compliance Team are actively working on establishing the data protection complaint process, in readiness.

6.3 As reported in the 2024/25 report, the ICO has established an Accountability Framework toolkit that enables organisations to self assess the extent that current policies and processes meet their expectations. This has been completed and built on to provide a prioritised and risk based work programme for the SIGB and its working groups, and is monitored alongside other information related compliance frameworks, such as the NHS Data Security and Protection Toolkit. The Framework is broken down into the following ten categories:

i) Leadership and oversight;

ii) Policies and Procedures;

iii) Training and Awareness;

iv) Individuals Rights;

v) Transparency;

vi) Records of Processing and Lawful Basis;

vii) Contracts and Data Sharing;

viii) Risks and Data Protection Impact Assessments;

ix) Records Management and Security; and

x) Breach Response and Monitoring

6.4 The action plan is included as Appendix B to this report. Progress has been slower than hoped, as the OIGG are owners of the majority of actions, and have had a challenging agenda due to the level of business change (in particular the need to review Data Protection Impact Assessments). Similarly there have been pressures on the supporting teams with delivery sitting with a small number of professional officers, such as that of the Data Protection Officer, the Cyber Security and ICT Continuity Lead, and the Data and Information Manager. The recruitment of a temporary Data Protection Analyst has been completed (subject to successful references), and it is hoped that during their 12 month tenure there will be an improved movement on outstanding actions. The Priority One actions are noted below:

- 02c: Develop a Power BI Policy
- 02e: Develop Data Protection Complaints process
- 03a: Develop and roll out information governance training matrix
- 03f: Roll out RIPA / covert surveillance training
- 06a: Roll out of Information Asset Register
- 08d: Support Our Future Council transformation programme with information governance input
- 09a: Workstream to design digital records procedures (“simplifying records management”)
- 09e: Revise access control policy

- 10a: Strengthening data breach recording mechanisms and risk assessment tool

7. Alternative options considered

7.1 None

8. Legal considerations

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

9. Financial implications

9.1 There are no direct financial implications from this report. However, the General Data Protection Regulations set 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.

10. Natural environment, climate & ecology implications

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

11. Well-being and health implications

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

12. Other implications

12.1 None

13. Risk implications

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

Current Risk: High
Residual Risk: High

13.2 This scoring reflects the four high risks specified in section 5.6 of the report. There are also challenging resourcing demands in implementing the action plan at Appendix B.

14. Equalities

14.1 None

15. Appendices

Appendix A – Background information – Information Governance Structures

Appendix B – Information Governance Action Plan

16. Background papers

None

17. Report sign-off

17.1 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)

Appendix A

Information Governance Structures at Dorset Council

Information governance at Dorset Council can be broadly split into three main areas: i) information compliance (including data protection, information requests and regulation of investigatory powers); ii) information security (including cyber threats); and iii) information management. This is set out in more detail in the Information Governance Policy.

The Assurance Team includes a statutory Data Protection Officer (DPO). Whilst employed by the Council (and working to the Service Manager for Assurance), the UK General Data Protection Regulations require that the DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level. This link is provided by the Assurance Service reporting to the Director for Legal and Democratic, who acts as the Senior Information Risk Owner (SIRO) and the conduit with the Senior Leadership Team (SLT).

The SIRO role is mandatory for public sector organisations and is responsible for implementing and managing information risks within the organisation.

The role of Caldicott Guardian is performed by the Corporate Director for Adult Social Care Operations. This is a statutory role, responsible for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately. Key responsibilities are to act as the 'conscience' of the organisation and champion confidentiality issues with senior management; provide leadership and informed guidance on complex matters involving confidentiality and information sharing; and ensure that the council satisfies the highest practical standards for handling personal information.

The Council established a Strategic Information Governance Board (SIGB) late 2022, chaired by the SIRO with representatives from all Directorates that sit on their respective management teams. Professional advice is provided to the SIGB by a range of officers (DPO, Caldicott Guardian, information management, cyber security, business intelligence, legal, human resources; and the transformation programme). The SIGB has authority to approve information governance policies, practices and standards developed by the operational groups. The board also has authority to accept risk or enable appropriate controls to bring the risk down to an acceptable level, escalating to the SLT at the SIRO's discretion. Recognising that loss of data is a key component of the fraud risk, the board's remit has been extended to provide an overview of fraud management arrangements.

The SIGB is supported by a number of operational working groups. These groups will commission separate task and finish groups to undertake particular focussed work as necessary.

Operational Information Governance Group (OIGG)

Chaired by the Service Manager for Assurance, as the name suggests this Group has responsibility for operational information governance matters. This includes i) review and development of policies, processes and standards; ii) response to adverse performance; iii) monitoring of service information governance risks; iv) review and challenge of Data Protection Impact Assessments; and v) monitoring the roadmap of legislative change. The OIGG is identified as a consultee within the Our Future Council transformation programme.

Organisational Compliance and Risk Learning Group

This is chaired by the Strategic Performance Intelligence and Risk Officer with a remit for debriefing information related risk events that occur so that learnings can be agreed and cascaded/communicated. The Group also has a lead role in identifying and commissioning audits on information governance activities.

Cyber Security Technical Group

Chaired by the Cyber Security and ICT Continuity Lead this group provides the operational capabilities for cyber security and ICT within the Council, in addition to the response and recovery to an incident.

Digital Applications Governance Group

This was previously chaired by a Programme Manager in the Transformation, Innovation and Digital Service, but has been decommissioned and replaced by the Internal Technical Design Authority as part of the Our Future Council programme. Its former role had been to monitor the roadmap of Microsoft applications, alongside other system developments, and reviews business requests for accepting applications into the Council's ICT infrastructure, with an analysis of risk (data protection / cyber security / information risk) vs business opportunity. An action has been identified to look at whether the decommissioning results in gaps that need to be picked up by the other task and finish groups.

Appendix B – Information Governance Action Plan

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
01a	Develop an Information Governance resourcing plan	1) Leadership & Oversight	Operational	Priority 1	SM for Assurance / DPO	Completed
01b	Review intranet guidance and / or develop SharePoint Hub	1) Leadership & Oversight	Operational	Priority 2	DPO	
01c	SIGB to review effectiveness of existing operational sub groups	1) Leadership & Oversight	Strategic Information Governance Board	Priority 2	SIGB and Chairs	Operational Information Governance Group has carried out a review.
02a	Develop schedule of policies and prioritised review dates, integrating into corporate template	2) Policies & Procedures	Operational	Priority 1	SM for Assurance / DPO / ICT Cyber Security Lead	Completed
02b	Refresh policy framework regarding processing of special category/criminal offence data	2) Policies & Procedures	Operational	Priority 2	DPO	
02c	Develop Power BI policy	2) Policies & Procedures	Operational	Priority 1	Head of Strategy	This has been drafted, pending sign off.

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
02d	Review overarching Data Protection policy	2) Policies & Procedures	Operational	Priority 2	DPO	
02e (New)	Develop data protection complaints policy and supporting process	2) Policies & Procedures	Operational	Priority 1	DPO	
03a	Develop and roll out Information Governance training matrix	3) Training & Awareness	Operational	Priority 1	SM for Assurance	Training sub group established and criteria for matrix identified. Rolling out to Directorates for data gathering
03b	Determine mechanisms for delivery of training for high risk roles / service areas (following completion of training matrix)	3) Training & Awareness	Operational	Priority 3	DPO / ICT Cyber Security Lead	
03c	Develop communications plan with corporate communications team, with periodic IG reminders	3) Training & Awareness	Operational	Priority 2	SM for Assurance / DPO	Completed. Periodic items have now been agreed within the training calendar
03d	Development and delivery of induction training for elected members of data	3) Training & Awareness	Cyber Security;#Operational	Priority 1	DPO / Cyber Security Lead	Completed

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
	protection / cyber security					
03e	Review content of existing information governance training modules	3) Training & Awareness	Operational	Priority 3	DPO	This will be undertaken by the training sub group
03f	Roll out RIPA / Covert Surveillance training	3) Training & Awareness	Operational	Priority 1	SM for Assurance / DPO	The training has not yet been delivered to support the approved Covert Surveillance policy
04a	Strengthen processes to support individual requests for data erasure, with appropriate audit regime, in accordance with article 17	4) Individuals Rights	Operational	Priority 4	DPO	
04b	Review and update Individuals Rights policy	4) Individuals Rights	Operational	Priority 4	DPO	
05a	Review public schedule of privacy notices, identifying purposes of the processing and legal basis and ensure	5) Transparency	Operational	Priority 4	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
	process for review and update					
05b	Incorporate privacy information into the mandatory data protection training	5) Transparency	Operational	Priority 3	DPO	
06a	Roll out of Information Asset Register	6) ROPA & Lawful Basis	Operational	Priority 1	Information Management / DPO; input from all services	Partially complete. External introductory IAO training delivered in Feb 2025. In-house training content now being developed by RM and OD, including e-learning modules. This will facilitate launching a self-directed approach for managers to contribute to the IAR.
07a	Develop Data Sharing policy, with Information Asset Register providing mechanism for logging agreements and identifying gaps	7) Contracts & Data Sharing	Operational	Priority 1	DPO	Completed
07b	Development of third party supply chain risk management framework	7) Contracts & Data Sharing	Operational	Priority 3	DPO	Audit questionnaire being developed via OIGG

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
08a	Reflect information risk into the overarching Data Protection policy, linked to Information Asset Register work	8) Risks & DPIAs	Operational	Priority 4	DPO / Information Management	
08b	Finalise and roll out revised Data Protection Impact Assessment guidance, with centralised log	8) Risks & DPIAs	Operational	Priority 2	DPO	Good progress, and “show and share” for staff is imminent
08c	Develop DPIA training process	8) Risks & DPIAs	Operational	Priority 3	DPO	
08d	Support Our Future Council transformation programme with information governance input	8) Risks & DPIAs	Operational	Priority 1	DPO / OIGG	Governance arrangements established, and OIGG included as a consultee
09a	Workstream to design digital records' procedures (Simplifying Records Management)	9) Records Management & Security	Records Management Project	Priority 1	Information Management / User Adoption	Business case drafted to focus on migrating necessary information from shared drives, resource request to be taken to Senior Leadership Team in June 2025

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
09b	Improve Self-Service Portal, the paper records tracking system for the Records Management Unit	9) Records Management & Security	Records Management Project	Priority 3	ICT / Information Management	Completed
09c	Implement Data and Technology Strategy	9) Records Management & Security	Organisational Compliance & Risk Learning Group	Priority 3	Head of Strategy	
09d	Revise Acceptable Use policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead	Completed
09e	Revise Access Control policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead	Identified within 2023 SWAP audit on Data Quality and Information Governance
09f	Establish working group to look at the risks associated with WhatsApp and other similar social media messenging facilities	9) Records Management & Security	Operational	Priority 2	SM for Assurance / DPO and working group	
09g	Implement process of clear desk checks	9) Records Management & Security	Organisational Compliance & Risk Learning Group	Priority 4	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
09h	Refresh of business continuity plans, with transfer of action cards to MS Teams, and focus on data loss	9) Records Management & Security	Operational	Priority 1	SM for Assurance / Emergency Planning	Completed
09i	Roll out of Cyber business continuity exercises	9) Records Management & Security	Operational	Priority 1	Emergency Planning	Completed
09j	Develop AI policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead / DPO	Completed
09k	Develop Account Activity Policy	9) Records Management & Security	Operational	Priority 2	ICT Cyber Security Lead	Completed
10a	Strengthen data breach recording mechanisms and risk assessment tool	10) Breach Response & Monitoring	Operational	Priority 1	DPO / Asst DPO	
10b	Strengthen the lessons learnt process and ownership within service areas for low level breaches (ie those not considered by Risk and Learning Group	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 2	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
10c	Develop audit plan for information governance compliance audits and reporting process	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 3	Head of Strategy / DPO	
10d	Review and improve range of Information Governance KPIs	10) Breach Response & Monitoring	Operational	Priority 1	SM for Assurance / DPO	Completed
10e	Work with ICT colleagues in the roll out of E5 to explore mechanisms to reduce data breaches and cyber exposures	10) Breach Response & Monitoring	Operational	Priority 1	DPO / ICT Cyber Security Lead	Completed
10f	Develop formal process for recording and tracking actions resulting from data / cyber breaches	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 2	Head of Strategy/ DPO	
10g	Review and update Data Breach policy	10) Breach Response & Monitoring	Operational	Priority 2	DPO	