# Audit and Governance Committee
# 22 July 2024
# Annual Information Governance Report

## For Review and Consultation


**Portfolio Holder:** Cllr N Ireland, Leader and Cabinet Member for Governance, Performance, Communications, Environment, Climate Change and Safeguarding

**Executive Director:** J Mair, Director of Legal & Democratic

Report Author: Marc Eyre
Job Title: Service Manager for Assurance
Tel: 01305 224358
Email: marc.eyre@dorsetcouncil.gov.uk

Report Author: James Fisher
Job Title: Data Protection Officer
Tel: 01305 838125
Email: james.fisher@dorsetcouncil.gov.uk


**Report Status:** Public


**Brief Summary:** This is the second Annual Information Governance Report and sets out the progress made during 2023/24 in further embedding information governance.


**Recommendation**: To note the 2023/24 activity and focus for 2024/25.

**Reason for Recommendation**: To ensure that information governance is embedded and effective across Dorset Council.

### 1 Information Governance Structures at Dorset Council

1.1 This is the second 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 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.

1.3 The report is supported by the 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).

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

1.5 The role of Caldicott Guardian is now performed by the Corporate Director for Adult Social Care Operations, having previously sat within Childrens Services. 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.

1.6 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.

1.7 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.

1.8 Operational Information Governance Group
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.

1.9 Organisational Compliance and Risk Learning Group
This is chaired by the Service Manager for Business Intelligence and Performance 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.

1.10 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.

1.11 Digital Applications Governance Group
This is chaired by a Programme Manager in the Transformation, Innovation and Digital Service. The group monitors the roadmap of Microsoft applications, alongside other system developments. It 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.

## 2 Information Governance Activity During 2023/24

2.1 Whilst established towards the end of 2022/23, the SIGB and its supporting working groups have been embedded more fully during 2023/24, to provide a really solid platform for assurance over information governance and challenge/testing of risk acceptance.

2.2 The Council's overarching Information Governance Policy was reviewed and refreshed in January 2024 by the SIGB. This policy outlines the strategic framework of individual responsibilities, accountable roles, governance groups, and cooperation between information-related professionals, to build a culture that values information as an asset.

2.3 The Records Management Policy was also reviewed and updated by the SIGB. This policy sets out Dorset Council's commitment to achieving high standards in records management in order to meet its strategic objectives, legislative and regulatory obligations, mitigate risk and adhere to best practice standards.

2.4 **Cyber Security**

2.4.1 The Information Commissioners Office released statistics highlighting that cyber attacks on local authority systems have increased by 24% between 2022 and 2023. Because of this inherent risk, the threat of a successful cyber attack is currently identified as an extreme risk in the Council's risk register. Cyber security has made steady progress over the last year. With some changes to technical systems being more of a lateral move initially but with the potential to offer significate improvements mid and long term. This includes replacing the existing Security Incident and Event Management (SIEM) solution with a new product.

2.4.2 Vulnerability management procedures have been improved reducing the time the council is exposed to technical flaws in software that can allow a successful cyber attack.

2.4.3 The way in which requests for new applications within the council has been improved both for larger line of business applications and for client based smaller applications. This work is not completed although a multi discipline project is underway to review Application Portfolio Management within the council.

2.4.4 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. At the time of writing this report whole authority compliance is at 73%.

2.4.5 A set of business continuity exercises are being distributed to services, to allow them to test their current resilience to both cyber attack and any resultant loss of data.

2.4.6 Despite these significant improvements, it is accepted that the impacts of a successful attack can be so significant that the risk level will always remain high. There are measures that the council does not currently have in place which could further reduce both the likelihood and impact of a successful attack. A discussion with senior political and officer leadership regarding our risk appetite would be welcome to ensure we achieve the strongest defensive posture possible within the context of the council's financial position.

2.5 The Council's Data and Business Intelligence Strategy was approved in February 2023. This 5-year strategy sets out to put using data at the heart of the Council's decision-making, and is an integral part of "Our Future Council" transformation. The Data and Business Intelligence programme includes a number of information governance related projects: i) Data Governance, including data policy and sharing; ii) Data Quality; and iii) Records Management.

2.6 The Data Quality project recognises that data quality is a key component of the organisations Data and Business Intelligence Strategy. Pilot work for the Data and BI strategy identified that data quality concerns are a barrier to successfully being able to join data sets and hence to derive greater insights. To date the project has focussed on improving the unique identifiers which are captured within our Adults and Childrens services case management systems (NHS numbers; Unique Property Reference Numbers). This work will be expanded to include further systems across the council.

2.7 **Records Management project**

2.7.1 The Simplifying Records Management workstream, which is designing an approach to managing digital records across their lifecycle, produced an initial report in January 2024. This research contributed to the case for improved M365 licences.

2.7.2 The Information Asset Register (IAR) and ownership approach was modified following service design research. The IAR is being populated by rolling out a Microsoft Form to service managers, after first meeting with senior managers to gain support. Information Asset Owner live training sessions and self-directed learning content is being developed.

2.7.3 Backlog paper records transfers have been physically processed and are available for request from the Records Management Unit (RMU). Project resource is now focused on storage areas not in the control of Records

Management, such as clearing ex-district council records from the G3 warehouse on the Marabout Industrial Estate.

2.7.4 The Children's retention schedule was reviewed, expanded and has new owners assigned.

2.7.5 For destructions, a new process was established to guide Information Asset Owners to approve disposal at the policy level rather than file-by-file. This is a risk-based approach to resolving the still-large destructions backlog and was endorsed by the SIRO. Currently transfers and destructions data remains on workaround spreadsheets. To improve the Self-Service Portal system tracking paper records, a service designer proposed requirements and this is awaiting ICT resource to implement.

2.8 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 satisfactorily completed in June 2024, but recognised that the Council was not meeting the mandatory requirements on data protection and cyber security training. As a result, the Council is subject to an action plan to improve compliance rates on mandatory training. The 2024 return was submitted 28 June 2024, noting an improvement in training rates but remaining below the 95% compliance rate. The risks associated with non-compliance with the toolkit are equally applicable to the Public Services Network and other ICT assurance frameworks.

2.9 A new "Use of Covert Surveillance" policy was approved in January 2024, 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 2023/24;
- The number of RIPA light authorisations requested and granted – One instance in 2023/24, where covert surveillance was adopted for a fraud investigation;

- 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

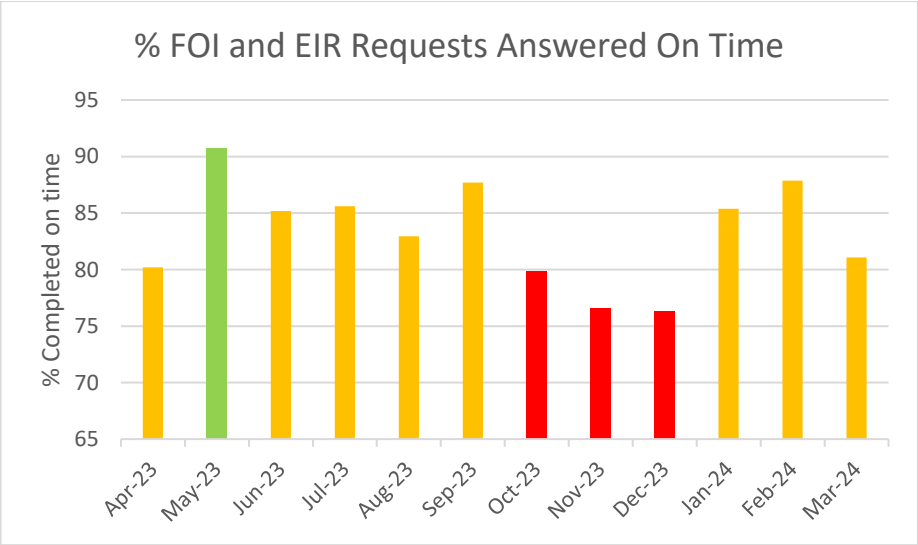
## 3 Performance and Risk

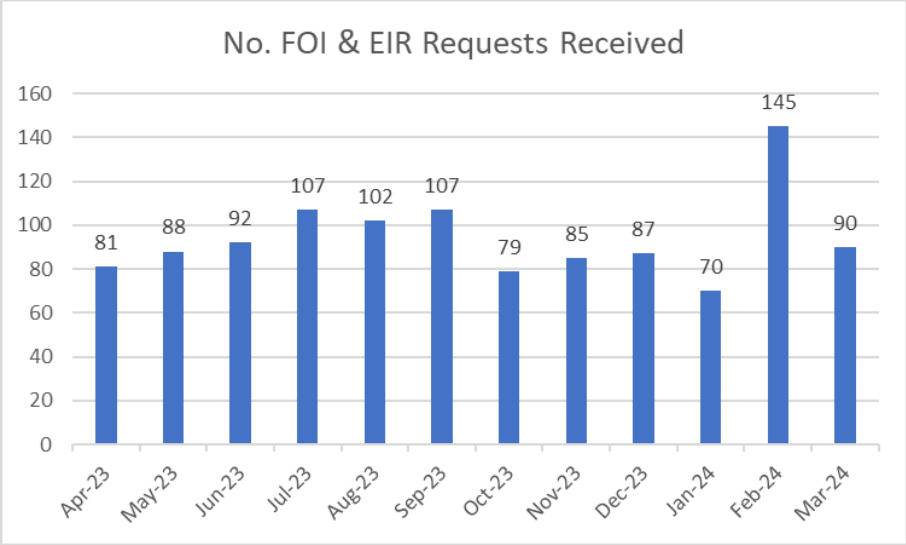
3.1 A range of performance indicators are monitored in respect of the Council's information compliance arrangements. These are not replicated in full here, but top level "whole Council" figures have been included.

### 3.2 Public and Environmental Information Requests

3.2.1 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 2023/24, the Council received 1,358 requests – approx. 113 per month.

3.2.2 The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. Whilst this was met in only one month during 2023/24, compliance exceeded 85% in six of the twelve months. Compliance dropped below 80% for the three months October to December 2023. With Freedom of Information request numbers on the increase, there is pressure on both the Information Compliance Team and responding services. As part of effort to manage this increase, the Council is currently exploring automation for some elements of the process.






### 3.3 Requests Relating to Personal Information

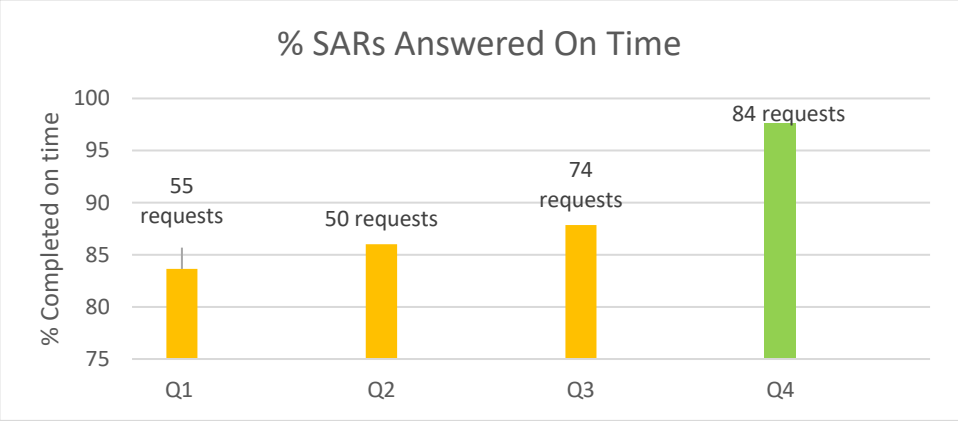
3.3.1 Individual Rights allows data subjects to enact certain powers over their personal information that is held. The most common and well known of these rights is the right of access, commonly referred to as subject access or subject access requests (SARs). This gives individuals the right to obtain a copy of their personal data held by an organisation, as set out in the General Data Protection Regulations. During 2023/24 the Council received 343 SARs. Of these, 266 became active, approx. 22 per month. Of these, 63% related to Childrens Services. 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. Since GDPR legislation became law in 2018, requests have increased at a rate of approximately 24% year on year, but this trend has recently plateaued.

3.3.2 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). Compliance was above 85% in three of the quarters and achieved 98% in quarter four. This is a significant achievement, as the complexity level of SARs has increased, with approx. 51% of request being deemed as 'complex' in nature and an extension being justified.

3.3.3 The improvement in performance has been achieved through an effective and efficient two stage review process, increased knowledge within the SAR team, and outsourcing of redactions where caseloads exceed

capacity. A business case has been approved to increase the internal SAR team by a further 0.5fte, to reduce outsourcing costs, and improve flexibility / resilience. Recruitment is underway for this post.

3.3.4 With this being said, requests that are deemed as 'very complex' and require the full two-month extension (for example the care leaver requests) are generally onerous to redact, and therefore exceeding 90% compliance for these requests will remain a challenge.




## 3.4 Data Breaches

3.4.1 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.

3.4.2 The 2023/24 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. Twenty of these incidents were determined by the Data Protection Officer to meet the criteria for escalation to the ICO. There has been no enforcement action by the ICO, but on a number of occasions recommendations have been made and

actions mandated. The causes of data breaches during 2023/24 are summarised below:

| Incident Category | Frequency in 2023/24 | % of recorded incidents |
|---|---|---|
| Email | 271 | 73% |
| Post | 27 | 7% |
| Failure to redact | 14 | 4% |
| Unauthorised internal access | 11 | 3% |
| Lost | 10 | 3% |
| Telephone | 9 | 2% |
| Other | 31 | 8% |

3.4.3 As can be seen from the figures above, 73% of breaches relate to the use of email. 70% of the email breaches relate to an incorrect email address being used; 16% relate to the wrong attachment being included; and 12% relates to inclusion of too many recipients. Email security is already a core part of the council's mandatory data protection and cyber security training for all staff. With recent changes to the Council's licencing arrangement with Microsoft, we plan to explore and introduce additional technological capabilities to help reduce the frequency and severity of email and other technology related data breaches. A working group is determining roll out priorities at this point in time, liaising with the Data Protection Officer as appropriate.

3.4.4 The Organisational Compliance and Risk Learning Group has been operating since the beginning of 2023/24. The role of this group is developing, but it 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 now reviews all data breach incidents that are reported to the ICO.

### 3.5 Mandatory Data Protection and Cyber Training

3.5.1 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 incorporated into the elected member induction programme, post elections.

3.5.2 Data protection compliance training has improved in the last twelve months, and currently sits at approx. 84%, but is still significantly short of the target 95%. The compliance levels for Cyber Security training are slightly lower, at 73%.

3.5.3 The Operational Information Governance Group has initiated a task and finish group to develop both a training matrix for higher risk role training needs and to further improve/refresh content.

3.6 The Council's risk register identifies 18 risks with an information governance focus, five of which are identified as "High" or "Very High" as set out in the table below:

| **Risk** | **Risk Ranking** | **Management Response** | **Risk Owner** |
|---|---|---|---|
| 213 - Failure to demonstrate evidence to support the NHS Digital Toolkit results in a lack of access to NHS data and systems | High | Satisfactory approval of the NHS toolkit is essential, for continued access to health data sets. The 24/25 return notes that data protection and cyber training is below the 95% compliance rate expected (currently circa 70-85%) and an improvement action plan has been initiated. Improving compliance rates and roll out of the training matrix are priorities for the training task and finish group. | Service Manager for Assurance |
| 286 - Loss of ICT service or data through a cyber-attack | 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. | Head of ICT Operations |

| Risk | Risk Ranking | Management Response | Risk Owner |
|---|---|---|---|
| | | Ongoing focus is on vulnerability management. In simple terms, this is a continuous, proactive process that helps keep computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. It involves identifying, assessing, and addressing potential security weaknesses to prevent attacks and minimise damage. The goal is to reduce overall risk exposure by mitigating as many vulnerabilities as possible. The implementation of vulnerability management technologies has led to an impressive 82% reduction in technical vulnerabilities on devices since introduction. This indicates that these technologies are effective in enhancing security.<br><br>The council's identity management system, which includes multifactor authentication, conditional access, and account permissions, has undergone a review. With the support of specialist technology, a significant number of vulnerabilities have been removed from the Council's systems. | |

| Risk | Risk Ranking | Management Response | Risk Owner |
|---|---|---|---|
| 348 - There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure. | Very High | An ICT service continuity exercise is currently being scoped. We are moving away from controlled power downs and prioritising core services and recovery testing. | Head of ICT Operations |
| 388 - Insufficient uptake of data protection training and inadequate awareness of statutory obligations | High | The mandatory data protection e-learning module was revised in early 2021. Compliance levels are currently circa 84% for staff. The e-learning has now been rolled out to elected members, to top up the data protection training received by members as part of induction. A training matrix has been established to identify any posts requiring more/less than the "benchmark" e-learning module. A training task and finish group has been established, working to the Operational Information Governance Group, with a focus on gaps in training, compliance and ensuring training fits job role/risk | Service Manager for Assurance |
| 321 - Unable to sustain | High | There are significant pressures on the information compliance team, with an increase in | Service Manager for Assurance |

| Risk | Risk Ranking | Management Response | Risk Owner |
|---|---|---|---|
| Assurance service due to prolonged pressures (increasing caseloads etc), changing legislative demands and gaps in staff capacity | | reported data breach cases and Freedom of Information, increasing complexity of Subject Access Requests and service demands for data protection support.<br><br>Transformation work is impacting significantly on the demands of the Data Protection Officer. The Information Commissioners Office's Accountability Framework has been completed and identified a number of gaps in DC's arrangements, which will be resource hungry to resolve.<br><br>A review of caseloads is currently underway, and automation is being explored to assist with rising Freedom of Information requests. Future resource needs are being assessed. | |

## 4 Focus for 2024/25 – The ICO Accountability Framework

4.1 The Government has proposed reform changes to the existing data protection legislation. 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.

4.2 The ICO has established an Accountability Framework toolkit that enables organisations to self assess the extent that current policies and processes meet their expectations. Whilst noting that the changing legislative framework may alter some of the ICO's expectations in the long term, the Operational Information Governance Group is in the process of completing this self assessment. It is envisaged that this will provide a prioritised and risk based work programme for the SIGB and its working groups, and can be 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

4.3 The self assessment for Dorset Council is summarised within the graph below. Where noted as "blank", this recognises that the self assessment has not yet been completed:

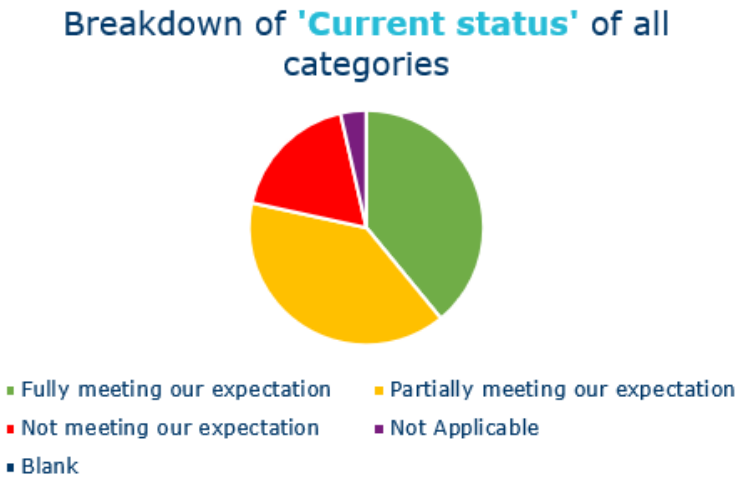



*Fig1 – Proportion of assessment criteria where Dorset Council meets ICO expectations*

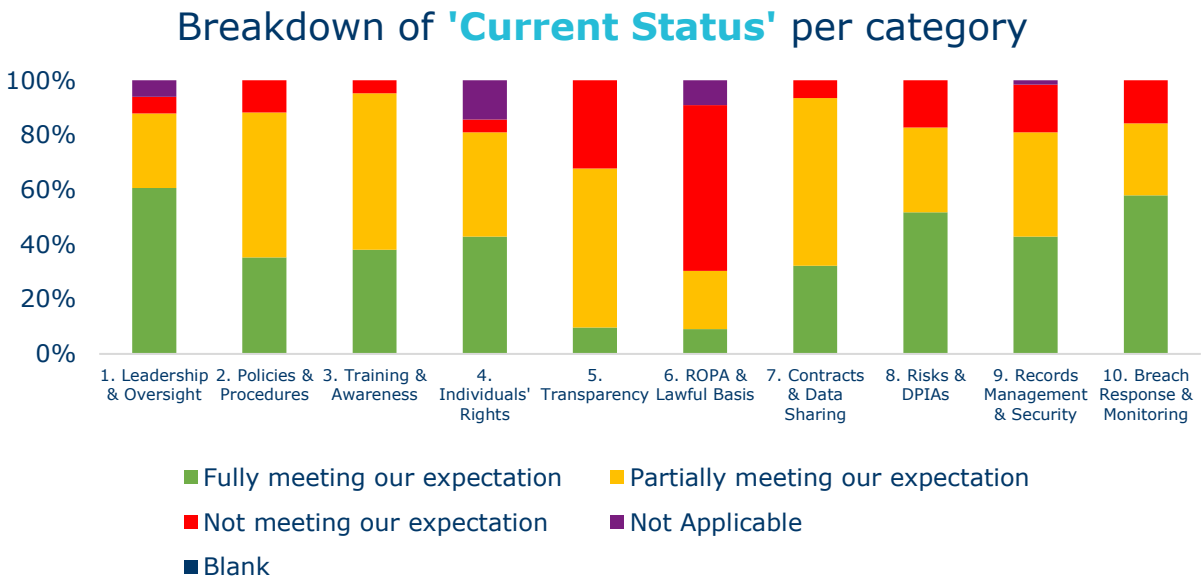



*Fig 2 – Proportion of assessment criteria where Dorset Council meets ICO expectations, per category.*

4.4 The self assessment identifies that the Council is not fully meeting the ICO's expectations for over 50% of the criteria. In general, the Council scores higher for physical controls, but less well in terms of the application and embeddedness of processes necessary to support strong information governance practices. The Operational Information Governance Group has developed a risk based prioritised action plan for adoption by the SIGB, which is set out in Appendix A. However it is recognised that this is

a challenging agenda, which is likely to determine additional resourcing needs. Delivery is likely to sit 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, which may present resourcing implications to deliver improvement within acceptable timescales. Particular findings are noted below.

4.5 **Leadership and Oversight –** The set up of the Strategic Information Governance Board and its associated operational groups provide a positive framework for information governance, with clearly defined roles and escalation to SLT. There are resource shortfalls for what is a challenging agenda to fully meet ICO expectations. **Key actions for 2024/25 –** Development of a resourcing plan, for consideration by Strategic Information Governance Board.

4.6 **Policies and Procedures –** A set of policies were established for Day One of Dorset Council and a number of these have not yet been reviewed and updated to ensure that they remain fit for purpose. **Key actions for 2024/25 –** Development of Data Sharing Agreement and AI policies; develop prioritised workplan for wider policy reviews, including identification of gaps in existing policy framework, as part of the Data Governance project.

4.7 **Training and Awareness –** Data protection and cyber security training are mandatory for all staff and councillors. However compliance rates are not currently at the required level. Work is underway to develop a training matrix to determine higher risk staff roles that should be subject to a more "job specific" training. **Key actions for 2024/25 –** Finalise and rollout training matrix and update on training modules.

4.8 **Individual Rights -** This relates to an individual's right to access to information about them, the right to rectification, erasure and restriction of processing. Good progress has been made in improving compliance rates for subject access requests.

4.9 **Transparency -** This category covers the content and effectiveness of privacy notices – a requirement under UK GDPR setting out how a person's information is held and used. The combined Information Asset Register and Record of Processing Activities (ROPA) is in the process of rollout, and will be a foundation for information privacy review. **Key actions for 2024/25 –** Roll out of Information Asset Register, including

training programme for Information Asset Owners; enable process for review and update across services.

4.10 **Records of Processing and Lawful Basis –** The combined Information Asset Register and ROPA is in the process of rolling out, and a training programme is in place to support Information Asset Owners to submit and manage entries to the register. **Key actions for 2024/25 –** Roll out of Information Asset Register, including training programme for Information Asset Owners.

4.11 **Contracts and Data Sharing –** A SWAP audit released in April 2023 found that the Council does not currently have a data sharing policy or framework, and that there is limited oversight. Information will be gathered about current data sharing agreements as part of the Data Governance Project and linked to the Information Asset Register. **Key actions for 2024/25 –** Identification and logging of data sharing agreements; development of data sharing policy; development of third party supply chain risk management framework.

4.12 **Risks and Data Protection Impact Assessments (DPIA) –** "Data protection by design and default" is a key element of ensuring that service delivery change reflects a review of data protection implications. The Council has a process for impact assessments, but is currently being enhanced. The transformation programme incorporates the requirement for DPIAs. DPIAs are reviewed and signed off by the Operational Information Governance Group, but this does put a strain on other key items in the action plan. **Key actions for 2024/25 –** Finalise revised DPIA policy.

4.13 **Records Management and Security –** This category examines how we manage and secure both paper and digital information. The Simplifying Records Management workstream will design how best to respond to the gaps identified in digital records management. The benefits of good records management are savings in digital storage and greater efficiency for officers' day-to-day work. **Key actions for 2024/25 –** Records Management Project: improving our paper records tracking system, identifying uncontrolled paper records and arranging transfer into RMU, taking a resource request to Children's Services to resolve indexing and retention issues, producing user guidance and best practice recommendations on M365 storage and migrating from shared drives; collaborating on processes to maintain and review the IAR; review of the Acceptable Use policy; rollout of cyber business continuity exercises.

4.14 **Breach Response and Management –** There are clear processes for managing breaches. The Organisational Compliance and Risk Learning Group is assessing the most significant breaches. **Key actions for 2024/25 –** Implement improved lessons learnt process within Directorates, including lines of accountability; develop risk based information governance audit plan.

## 5 Financial Implications

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.

## 6 Natural Environment, Climate & Ecology Implications

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

## 7 Well-being and Health Implications

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

## 8 Other Implications

None

## 9 Risk Assessment

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

Current Risk: High
Residual Risk: High

This scoring reflects the five high risks specified in section 3.6 of the report. In particular, there are challenging resourcing demands in implementing the action plan at Appendix A.

## 10 Equalities Impact Assessment

Information Governance policies have been subject to Equalities Impact Assessments

## 11 Appendices

None

## 12 Background Papers

None

## 13 Report Sign Off

13.1 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 Action Plan

| Ref | Identified action | ICO Framework Category | By Whom / Sub Group | Risk based priority | Resourcing Requirements | Target Timescale | Latest Status |
|---|---|---|---|---|---|---|---|
| 1a | Develop an Information Governance resourcing plan | Leadership and Oversight | Operational | High | SM for Assurance / DPO | Priority 1 | |
| 1b | Review intranet guidance and / or develop SharePoint Hub | Leadership and Oversight | Operational | Medium | DPO | Priority 2 | |
| 1c | SIGB to review effectiveness of existing operational sub groups | Leadership and Oversight | SIGB | Medium | SIGB and Chairs | Priority 2 | |
| 2a | Develop schedule of policies and prioritised review dates, integrating into corporate template | Policies and Procedures | Operational | High | SM for Assurance / DPO / ICT Cyber Security Lead | Priority 1 | Schedule completed |
| 2b | Refresh policy framework regarding processing of special category/criminal offence data | Policies and Procedures | Operational | Medium | DPO | Priority 2 | |
| 2c | Develop Power BI policy | Policies and Procedures | Operational | High | SM for Business Intelligence | Priority 1 | |
| 2d | Review overarching Data Protection policy | Policies and Procedures | Operational | Medium | DPO | Priority 2 | |
| 3a | Develop and roll out Information Governance training matrix | Training and Awareness | Operational | Medium | SM for Assurance | Priority 1 | Training sub group established and criteria for matrix identified. Rolling out to Directorates for data gathering |
| 3b | Determine mechanisms for delivery of training for high risk roles / service areas (following completion of training matrix) | Training and Awareness | Operational | Medium | DPO / ICT Cyber Security Lead | Priority 3 | |
| 3c | Develop communications plan with corporate communications | Training and Awareness | Operational | Medium | SM for Assurance / DPO | Priority 2 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | team, with periodic IG reminders | | | | | | |
| 3d | Development and delivery of induction training for elected members of data protection / cyber security | Training and Awareness | Operational / Cyber Security | High | DPO / Cyber Security Lead | Priority 1 | Built into the May inductions |
| 3e | Review content of existing information governance training modules | Training and Awareness | Operational | Medium | DPO | Priority 3 | |
| 3f | Roll out RIPA / Covert Surveillance training | Training and Awareness | Operational | High | SM for Assurance / DPO | Priority 1 | The training has not yet been delivered to support the approved Covert Surveillance policy |
| 4a | Strengthen processes to support individual requests for data erasure, with appropriate audit regime, in accordance with article 17 | Individuals Rights 4.7.4 | Operational | Low | DPO | Priority 4 | |
| 4b | Review and update Individuals Rights policy | Individuals Rights | Operational | Low | DPO | Priority 4 | |
| 5a | Review public schedule of privacy notices, identifying purposes of the processing and legal basis and ensure process for review and update | Transparency 5.1 | Operational | Low | DPO | Priority 4 | |
| 5b | Incorporate privacy information into the mandatory data protection training | Transparency 5.5 | Operational | Low | DPO | Priority 3 | |
| 6a | Roll out of Information Asset Register | ROPA and Lawful Basis | Operational | High | Information Management / | Priority 1 | Roll out has begun, but is phased. Due to be completed end 2024. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | DPO; input from all services | | |
| 7a | Develop Data Sharing policy, with Information Asset Register providing mechanism for logging agreements and identifying gaps | Contracts and Data Sharing 7.1 | Operational | High | DPO | Priority 1 | Drafted pending consultation and sign off by Strategic Information Governance Board in Sept 24 |
| 7b | Development of third party supply chain risk management framework | Contracts and Data Sharing 7.4 | Operational | Medium | DPO | Priority 3 | |
| 8a | Reflect information risk into the overarching Data Protection policy, linked to Information Asset Register work | Risks and DPIAs | Operational | Low | DPO / Information Management | Priority 4 | |
| 8b | Finalise and roll out revised Data Protection Impact Assessment guidance, with centralised log | Risk and DPIAs | Operational | High | DPO | Priority 2 | |
| 8c | Develop DPIA training process | Risk and DPIAs | Operational | Medium | DPO | Priority 3 | |
| 8d | Support Our Future Council transformation programme with information governance input | Risk and DPIAs | Operational | High | DPO / OIGG | Priority 1 | Ongoing support |
| 9a | Workstream to design digital records' procedures (Simplifying Records Management) | Records management and security | RM Project | High | Information Management / User Adoption | Priority 1 | Current RM Project workstream is to design / deliver user guidance and best practice recommendations, and design the approach to migrating data, which is not currently resourced |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9b | Improve Self-Service Portal, the paper records tracking system for the Records Management Unit | Records management and security | RM Project | High | ICT / Information Management | Priority 3 | Awaiting ICT development resource |
| 9c | Implement a data quality policy and supporting processes | Records management and security | Org Compliance & Risk Learning | Medium | SM for BI | Priority 3 | |
| 9d | Revise Acceptable Use policy | Records management and security | Operational | High | ICT Cyber Security Lead | Priority 1 | In progress |
| 9e | Revise Access Control policy | Records management and security | Operational | High | ICT Cyber Security Lead | Priority 1 | Identified within 2023 SWAP audit on Data Quality and Information Governance |
| 9f | Establish working group to look at the risks associated with WhatsApp and other similar social media messenging facilities | Records management and security | Operational | Medium | SM for Assurance / DPO and working group | Priority 2 | |
| 9g | Implement process of clear desk checks | Records management and security | Org Compliance & Risk Learning | Low | SM for BI / DPO | Priority 4 | |
| 9h | Refresh of business continuity plans, with transfer of action cards to MS Teams, and focus on data loss | Records management and security | Operational | Medium | SM for Assurance / Emergency Planning | Priority 1 | Transfer to MS Teams complete. Gradual engagement across DC services |
| 9i | Roll out of Cyber business continuity exercises | Records management and security | Operational | Medium | Emergency Planning | Priority 1 | Exercise developed and rolled out |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9j | Develop AI policy | Records management and security | Operational | High | ICT Cyber Security Lead / DPO | Priority 1 | |
| 10a | Strengthen data breach recording mechanisms and risk assessment tool | Breach Response and Monitoring | Operational | Medium | DPO / Asst DPO | Priority 1 | Process agreed in principle |
| 10b | Strengthen the lessons learnt process and ownership within service areas for low level breaches (ie those not considered by Risk and Learning Group | Breach Response and Monitoring | Org Compliance & Risk Learning | Medium | DPO | Priority 2 | |
| 10c | Develop audit plan for information governance compliance audits and reporting process | Breach Response and Monitoring | Org Compliance & Risk Learning | Medium | SM for BI / DPO | Priority 3 | |
| 10d | Review and improve range of Information Governance KPIs | Breach Response and Monitoring | Operational | Medium | SM for Assurance / DPO | Priority 1 | Effective wef May 24 |
| 10e | Work with ICT colleagues in the roll out of E5 to explore mechanisms to reduce data breaches and cyber exposures | Breach Response and Monitoring | Operational | High | DPO / ICT Cyber Security Lead | Priority 1 | Agreed set up of M365 working group. Revised sensitivity labels agreed, subject to sign off |
| 10f | Develop formal process for recording and tracking actions resulting from data / cyber breaches | Breach Response and Monitoring | Org Compliance & Risk Learning | Medium | SM for BI / DPO | Priority 2 | |
| 10g | Review and update Data Breach policy | Breach Response and Monitoring | Operational | Medium | DPO | Priority 2 | |
| | | | | | | | |