Audit and Governance Committee
17 July 2023
Annual Information Governance Report

For Review and Consultation

Portfolio Holder: Cllr S Flower, Leader of the Council

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 first Annual Information Governance Report and sets out the progress made during 2022/23 in further embedding information governance. In particular the report highlights the role of the new Strategic Information Governance Board (SIGB) and its supporting operational working groups.

A self assessment has been undertaken using the Information Commissioners Office's (ICO) Accountability Framework. This maps current practices, policies and processes against the expectation of the ICO. The output of the self assessment presents a challenging agenda for the SIGB, but also recognises that a number of improvement measures are already underway, with ongoing projects relating to records management, the information asset register and managing information requests. The output from the self-assessment will be used to develop a risk based and prioritised work programme for the SIGB.

Recommendation: To note the 2022/23 activity and focus for 2023/24.

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 first 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 Leader of the Council holds the portfolio that includes information governance.

1.6 During the lead up to unitary status, an Information Governance Board was established as part of the Shaping Dorset Council programme, to ensure that appropriate information governance arrangements existed from day one. It was chaired by the SIRO.

1.7 The Cyber 360 Review undertaken during 2022 included a number of findings relating to the Board’s set up:

- That the role and remit of the Information Governance Board should be reviewed, including roles, lines of responsibility, approval paths, accountability, the management of resources, membership and frequency; and

- Dorset Council Management consider how lessons are identified and learnt in their review of the current governance arrangements and the scope of the Information Governance Board.

1.8 The Information Governance Board set up a task and finish group to respond to these findings. In particular, the Board had found the extent of business it faced challenging, with a wide remit that covered both operational and strategic issues. A report was considered and approved by SLT on 22 September 2022 which agreed the following:

- The Board would be disbanded and replaced by a Strategic Information Governance Board (SIGB), chaired by the SIRO with representatives from all Directorates that sit on their respective management teams. Professional advice to the SIGB to be provided by a range of officers (DPO, Caldicott Guardian, information management, cyber security, business intelligence, legal, human resources; and the transformation programme);

- Operational issues will be delegated to a number of working groups, with escalation to the SIGB as appropriate. The working group chairs will sit on the SIGB;

- The SIGB has authority to approve information governance policies, practices and standards developed by the operational groups;

- The SIGB has authority to accept risk or enable appropriate controls to bring the risk down to an acceptable level. Escalation to SLT would be at the SIRO’s discretion. Directorate representatives would ensure key messages are shared with Directorate Management Teams; and

- The SIRO will report to SLT on information governance on an exception basis, but at least once annually via the annual Information Governance report. This report will also be presented to Audit and Governance Committee.

1.9 The standing operational working groups for the SIGB are set out below. These groups will commission separate task and finish groups to undertake particular focussed work as necessary.

1.10 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; and iv) monitoring the roadmap of legislative change.

1.11 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 will also have a lead role in identifying and commissioning audits on information governance activities.

1.12 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.

1.13 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 2022/23

2.1 The key development during the last financial year was establishing the SIGB and its supporting working groups, which provides a really solid platform for assurance over information governance and challenge/testing of risk acceptance. All of the groups are now operational.

2.2 The Records Management project has a number of strands that will modernise the service's operations, most prominently to manage digital records. The "Simplifying Records Management for the Future" project will design an accessible, simplified approach to managing digital files on shared drives and in M365. Other workstreams are bringing paper records destructions and transfer backlogs up to date and establishing robust systems and processes. This includes improving the in-house system for day-to-day RMU operations and populating the Information Asset Register (IAR). The IAR tool will be launched alongside wider education on information ownership, to develop the essential Information Asset Owner role which provides assurance to the SIRO.

2.3 The findings of the Cyber 360 peer review were released in June 2022. This recognised that Dorset Council has in place a strong cyber security culture and very good general approach to cyber security. It identified evidence of capable leadership from SLT, demonstrated by high levels of personal engagement, robust relationships with IT and an enduring commitment to the appropriate funding of cyber security. A number of recommendations were identified, which are being tracked by the SIGB.

2.4 A Data and Business Intelligence Strategy was approved by Cabinet on 28 February 2023 setting out the council's ambition to place the use of data and intelligence at the core of decision-making and policy development. This strategy will inform the next phases of the council's development of information governance policies, processes and procedures, aiming to achieve systemic improvements to how information is collected, used and stored and the quality of our data. Strong data management and data quality are important to developing data analytic capabilities that allow the council to gain genuine insights from its data and make stronger predictions.

2.5 A risk assessment process has been developed and in use to assess risks and business benefits of any new applications prior to them being included within the Council's ICT infrastructure, reducing the risk of data loss/misuse or a cyber security incident.

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 Freedom of Information

During 2022/23, whole Council performance for Freedom of Information Requests responded to within timescales was recorded as Amber for 10 of the 12 months (three of which were very close to the 90% target), with December 23 and February 23 showing as Red (but still above 75%

compliance). The Information Compliance Team continue to provide regular management information to Directorates to improve their compliance rates.

3.3 Subject Access Requests (SARs)
Historically Dorset Council, and previously Dorset County Council, has struggled to comply with SAR timescales received in relation to children's social care. The number of SARs received has increased by approximately 24% every year. Whilst still falling generally below the 90% target, significant improvements have been made within the last twelve months. Childrens Services established a dedicated SARs team, and these transferred to Assurance in January 2022 to provide better alignment with other information compliance skillsets. As a result of this dedicated resource, and a review of processes and practices, the backlog of cases have now been largely processed.

3.4 SARs vary in complexity – it is a small number of very complex care leaver requests that largely drive the Red reporting. With the significant backlog now removed, it is envisaged that the performance will improve, but realistically responding to the most complex cases within timescales will remain a challenge. Cases above team capacity and/or deemed very complex are generally outsourced to an external provider, which has improved performance. A redaction software project is underway to look to improve process efficiency further.

3.5 Data Breaches
During 2022/23 four breaches were deemed significant enough to be escalated to the ICO, including details of the actions taken by the Council. In all four cases the ICO was content with the actions taken. This number is a reduction from five and six escalations in the preceding two years.

3.6 There were 168 confirmed breaches reported to the DPO in the last twelve months, in addition to 81 near misses. This compares to 136 and 142 confirmed breaches in the preceding two years. By far the largest cause of actual and/or potential breaches related to use of email (66%). Measures being taken to reduce this risk include greater control over the use of email distribution groups, improved visibility of the 'bcc' field within Outlook and data protection training to staff and councillors specifically covering the use of email.

3.7 Mandatory Data Protection Training
As at end of March 2023 mandatory data protection training compliance

was showing at 67%, measuring positively against 35% at the same point in 2022. However it remains significantly below 100%. The Operational Information Governance Group are looking at this further, including an analysis of higher risk roles that have not undertaken the training, which is being reported through to Directorates. The data has been compared with compliance rates for the mandatory cyber training, which highlights similar non-compliance with particular job groupings. 14% of individuals causing a data breach were found not to have completed the mandatory training in the last twelve months. This will remain a key area of focus for the operational group during 2023/24.

3.8 The Council's risk register identifies 17 risks with an information governance focus, four of which are identified as "High" or "Extreme" as set out in the table below:

Risk	Risk Ranking	Management Response	Risk Owner
286 - Loss of ICT service or data through a cyber-attack	Extreme	Vulnerability Management - The implementation of vulnerability management technologies has reduced by 82% since the introduction of vulnerability management technology. The council's identity management (multifactor, conditional access and account permission) has been reviewed with the support of specialist technology. A considerable number of vulnerabilities have been removed from the council identity management technologies. An external review of this technology is also being scoped.	Head of ICT Operations
348 - There is a business continuity risk from delayed ICT	Extreme	Scoping for the first exercise since LGR is being scoped. Controlled power down is no longer required so this exercise	Head of ICT Operations

Risk	**Risk Ranking**	**Management Response**	**Risk Owner**
recovery after a disruption such as a power failure.		will test core infrastructure services. Core services are the foundation of the recovery process and include the recovery procedure will be tested as part of the exercise to ensure it is fit for purpose.	
671 - Failure to issue DC email addresses to remote workers (passenger assistant and drivers) could result in a data breach under GDPR	High	Currently remote workers use their personal email addresses. There is a risk of a data breach as sensitive information may be sent to these personal addresses, which are often shared with other family members in the household. Remote workers also cannot access DC systems such as Learning Hub, Staff Intranet etc. therefore they cannot complete Corporate mandatory training, do not receive staff benefits, corporate emails (Employee news) etc. A project is underway to identify a solution, including a process of service redesign.	Head of Dorset Travel
393 - Inadequate "data protection by design and default" culture and processes	High	Work is necessary to embed a culture of Data Protection Impact Assessments for any transformational change proposals. A task and finish group has been established to look at developing a wider "Impact Assessment" tool, which would also embrace climate change and equalities impacts. This may need the	Service Manager for Assurance

Risk	Risk Ranking	Management Response	Risk Owner
		assistance of service based change champions to assist services with lower risk assessments. Higher risk impacts will be escalated to the Operational Information Governance group.	

3.9 Audit

South West Audit Partnership undertook an audit on "Data Quality and Information Governance" in the last quarter of 2022/23. The resultant level of assurance was noted as "limited". The report noted that positive progress has been made with the introduction of the SIGB and the approval of the Data and Business Intelligence Strategy. However, three "Priority Two" recommendations were made in respect of:

- Transfer of sensitive information to remote working staff cohort (see risk 671 above);
- Accuracy of Key Performance Indicator data recorded manually;
- Lack of a data sharing policy or framework and supporting library of agreements

3.10 The actions arising from this audit will be reflected within the SIGB action plan.

4 Focus for 2023/24 – 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 ICO accountability framework

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 provides a useful means of measuring the maturity of a relatively new Council's information governance arrangements, and build on this to provide a prioritised and risk based work programme for the SIGB and its working groups. This 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:

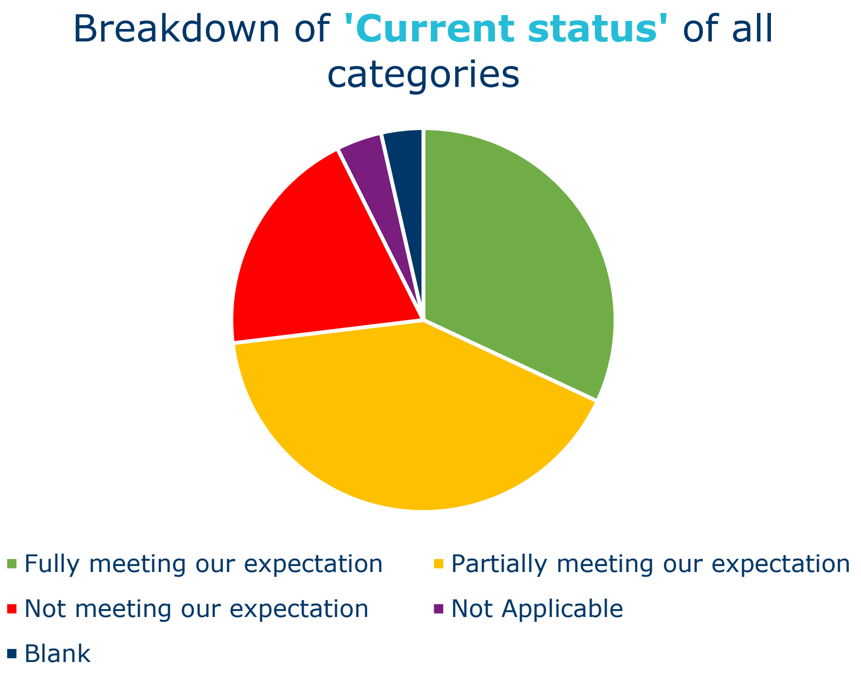

Fig1 – Proportion of assessment criteria where Dorset Council meets ICO expectations

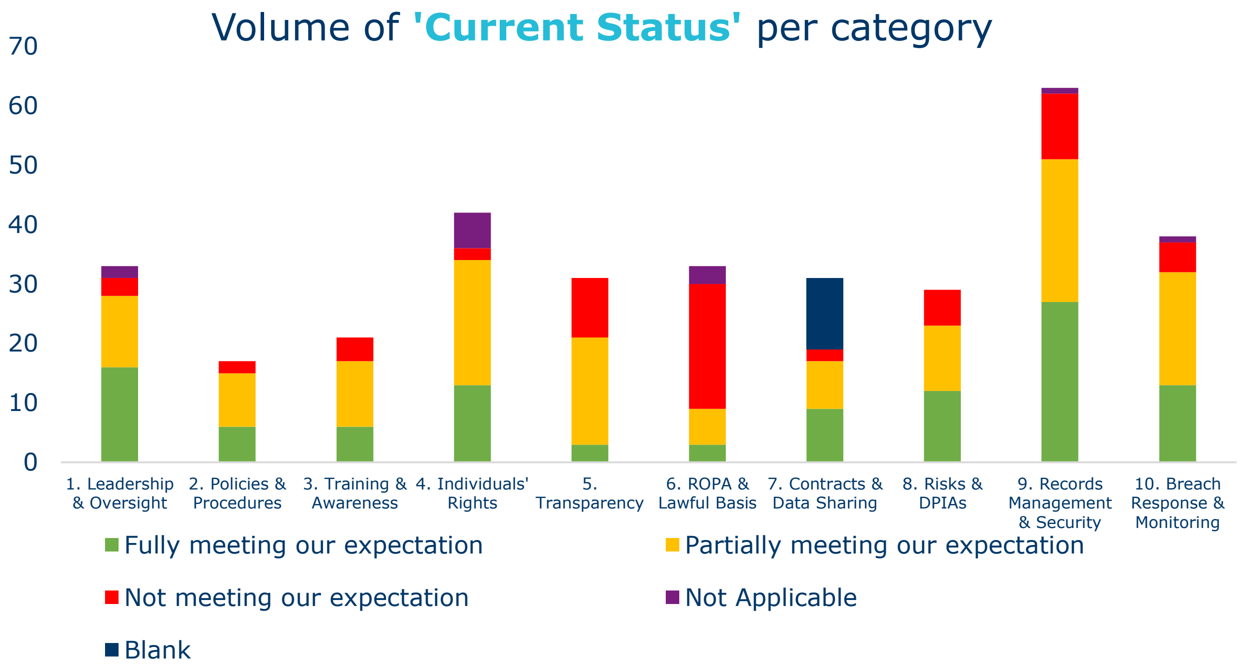

Fig 2 – Proportion of assessment criteria where Dorset Council meets ICO expectations, per category.

4.4 Whilst the self assessment identifies that the Council is either fully or partially meeting the ICO's expectations for 73% of the question set, there remains work to do to fully meet 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 priority focus for the Operational Information Governance Group for early 2023/24 will be to develop a risk based prioritised action plan for adoption by the SIGB. 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 and the Cyber Security and ICT Continuity Lead, 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. Further work is necessary to raise awareness around information governance. There are resource shortfalls for what is a challenging agenda to fully meet ICO expectations.

4.6 **Policies and Procedures –** A set of policies were established for Day One of Dorset Council but have not yet been reviewed and updated to ensure that they remain fit for purpose. The Operation Group will be establishing a priority order, incorporating also non-GDPR related policies, such as Regulation of Investigatory Powers and Freedom of Information. Data protection considerations into policy change more generally are not fully embedded.

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. Higher risk staff roles should be subject to a more "job specific" training, once a training matrix has been established.

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, but further work is required. This includes an ongoing redaction software project.

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. Further work is necessary to complete the Information Asset Register so that we can ensure the completeness and accuracy of privacy notices. Further work is required to understand the extent privacy notices are embedded into business processes. There is also a need to ensure that privacy notice wording is in clear and plain language.

4.10 **Records of Processing and Lawful Basis –** The information asset registers developed by predecessor councils have not yet been replaced by a Dorset Council register. A project is underway to progress this, but until the work is completed this category is largely showing as red.

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 of existing data sharing agreements. This will be a priority action for the Operational Information Governance Group.

4.12 **Risks and Data Protection Impact Assessments (DPIA) –** 4.10 above noted that work is underway to develop a Dorset Council information asset register. This will also act as a means of identifying significant information risks. "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 it is not sufficiently embedded. There will be a resource implication associated with responding to DPIA findings, and we need to be mindful of anticipated legislative change.

4.13 **Records Management and Security –** This category examines how we manage and secure both paper and electronic information. A records management project is currently underway which will respond to the majority of gaps identified.

4.14 **Breach Response and Management –** There are clear processes for managing breaches. The creation of the Organisational Compliance and Risk Learning Group will ensure that learning from breaches is more effectively identified and communicated. The Group will also respond to the auditing recommendations set out within this category.

4.15 Although outside of the ICO Accountability Framework work, as subject to a different regulator, the Council's policy for use of the Regulation of

Investigatory Powers (RIPA)is currently being reviewed and will be presented to a later meeting of this Committee for approval. RIPA is legislation governing the use of covert techniques by public authorities.

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

None

7 Well-being and Health Implications

None

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: Medium
Residual Risk: Medium

10 Equalities Impact Assessment

Information Governance policies have been subject to Equalities Impact Assessments

11 Appendices

None

12 Background Papers

None