Wiltshire Council
Where everybody matters

INFORMATION GOVERNANCE
SENIOR INFORMATION RISK OWNER ANNUAL REPORT
APRIL 2015 – MARCH 2016

1. PURPOSE

This report provides an overview of current Information Governance issues including compliance with key standards and a report on incidents. It ensures that CLT and Cabinet are advised of the most significant current and emerging Information Governance issues and the measures being taken by the Authority to ensure it meets the national and mandatory standards.

Specifically, this report will:

- Document organisational compliance with the legislative and regulatory requirements relating to the handling of information and provide assurance of ongoing improvement in relation to managing risks to information. This includes:
  - the Data Protection Act (1998)
  - the Freedom of Information Act (2000)
  - the Information Security Standard ISO/IEC 27002:2007
  - the Information Governance toolkit
- Detail any Serious Incidents Requiring Investigation (SIRI) within the preceding twelve months, relating to any losses of personal data or breaches of confidentiality.
- Report on the key achievements of the information governance improvement plan in 2015/2016 and to outline the next steps for 2016/2017.

2. RECOMMENDATIONS

That CLT and Cabinet:

- notes the content of this report and recognises the progress that has been made in the areas for improvement identified in the ICO's report together with the status of organisational compliance.
- considers the key risks associated with this programme and advises on the mitigations particularly with respect to the significant risk that the ICO has raised in respect to the sharing of councils' premises with other public bodies.
- agrees that this report with any amendments forms part of the council's annual governance statement to further improve information governance practices

3. BACKGROUND

In March 2015 the ICO were invited to conduct an audit of the Council's arrangements for the processing of personal data. The audit focused on records management; subject access requests and data sharing. The overall conclusion was that there was a limited level of assurance that processes and procedures are in place and delivering data protection compliance and that there is considerable scope for improvement.

An information Governance Board was established and an Information Governance Improvement Plan developed to address the areas for improvement.

The ICO audit identified a number of areas for improvement that led to an information Governance Board being established and an information governance improvement programme developed to address the recommendations in the ICO's report. Some have been targeted and implemented and some will form part of the future development plan.

The improvement programme is based on the NHS Information Governance Toolkit (version 13), which is recognised as providing a comprehensive set of standards for information governance and meets with the approval of the ICO. The Information Governance Toolkit is a performance tool produced by the Department of Health. It draws together legal rules plus central guidance and presents them in one place as a set of information governance requirements. The IG programme is supported by the programme office under the overall direction of the Senior Information Risk Owner (SIRO).

4. INFORMATION GOVERNANCE IMPROVEMENT PLAN

Good progress has been made in the areas for improvement identified in the ICO's report. An updated action plan was sent to the ICO in March 2016 and notice was received in April that the audit engagement is now complete. Actions have been identified and are in accordance with the requirements of the Information Governance Toolkit. A further implementation plan is being developed to ensure that all remaining actions are monitored and completed.

The ICO provided constructive feedback. Whilst it is acknowledged that some of the timescales have moved from the original plan, but the Board feel it is important that the organisation does not have a rapid, quick fix approach to put things right; but that there is the creation of a much more sustainable framework and strategy for Information Governance across the Council.

The current status of the programme is as follows:

4.1 Physical Records Storage

Records that were held in the Chapmans building in Trowbridge and at Churchfields in Salisbury have been purged and catalogued. There remains a requirement to purge records held elsewhere in the County and still held under old storage contracts. A project plan is being developed to rationalise and improve the Council's physical records storage arrangements and to consider the options for electronic storage for the future.

4.2 Information Governance Policies

A comprehensive suite of information governance policies has been drawn up, approved by the IG Board, the Corporate Leadership Team and published on the Intranet on a dedicated information governance site. Version control is managed strictly through the Information Governance Assurance Group. These include:

- Information Governance Framework
- Information Governance
- Privacy Impact Assessment
- Data Protection and Subject Access
- Freedom of Information
- Records Management
- Information Security
- Mobile Working
- Network Security
- Information Assets

Underpinning procedures and guidance are being prepared to sit under the policies and these will also be published on the intranet, which will be published and available by October 2016.

4.3 Future Development Plan

The follow-up report from the ICO demonstrated the number of actions that still require completion from the original audit in 2015:

Scope area	Number of recommendations in each scope area from the original audit report	Number of actions complete, partially complete and not implemented.
Records Management	35	6 Complete 12 Partially complete 16 Not implemented 1 Rejected
Subject Access Requests	28	1 Complete 7 Partially complete 20 Not implemented 0 Rejected
Data Sharing	16	0 Complete 6 Partially complete 8 Not implemented 2 Rejected
TOTAL COMPLETE **TOTAL PARTIALLY COMPLETE** **TOTAL NOT IMPLEMENTED** **TOTAL REJECTED**		**7** **25** **44** **3**

The Council is aware of the activities that need to be undertaken to complete and implement the remaining actions and these have also been included in the recent IGSoC return.

A summary of key activities is provided below:

ITEM / SUBSIDIARY PROJECT	PRPOPOSED DELIVERY TIMESCALE
Restructure of IG team	May 2016
Allocation of departmental co-ordinators for data protection/FOIs	June 2016
Communications plan for updating all staff of any changes	June 2016
Information asset leads identified	July 2016
Production of Information Risk Policy	September 2016
Information asset registers completed	September 2016
Establishment of KPIs for quarterly monitoring	September 2016
Underpinning procedures and guidance for all IG policies	October 2016
Training for remaining staff	November 2016
Records management review	March 2017
Transparency review	March 2017
Data protection process review	March 2017

There are several of existing council programmes that link with and will have significant impact on Information Governance – Single View of the Customer, Business Continuity, the new Procurement programme and strategy, ICT hardware refresh etc. The relevant Heads of Service will work together to ensure consistency of approach and that consideration is given to the relevant, cross cutting areas.

4.4 Governance

Dr Carlton Brand, Corporate Director, has been designated as the Senior Information Risk Owner (SIRO). An Information Governance (IG) Board and Information Governance Assurance Group (IGAS) have been established, and terms of reference have been drawn up for both groups.

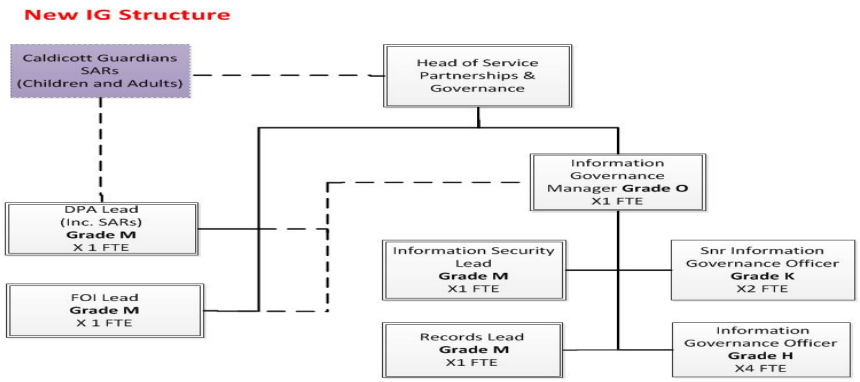
The IG Board is chaired by the SIRO and also includes the Caldicott Guardians for Childrens' and Adult Care; the council's Associate Directors for Legal and Governance; People and Business and Corporate Office, who is also a deputy SIRO; along with the Head of Partnerships and Governance also a Deputy SIRO, along with other senior officers. The IG Board is responsible for ensuring robust monitoring of the effectiveness of the Council's information governance arrangements and decision making relating to information governance.

The IGAS is chaired the Head of Partnerships and Governance and includes the new IG leads for data protection; FOI; information security and records management, as well as key Information Asset Owners. The IGAS will be responsible for reviewing practices across the council to ensure they are relevant and fit for purpose.

4.6 Restructuring of Information Governance Function

A new Information Governance team structure has been developed (in consultation with information governance experts, Dilys Jones Associates Ltd)

The team will sit within the Corporate Function, Procurement and Programme Office (CO).. The new structure has been designed to provide resilience and better strategic oversight of the 4 key areas of Information Governance.



4.7 Communications and Training Programme

The success of the improvement programme is dependent on changing the culture of the organisation so that staff have a clear understanding of the importance of good information governance, their responsibilities within their areas of operation and across the Council as a whole, and the need to discharge these diligently as an integral part of their day to day work.

A training programme for Corporate and Associate Directors, Caldicott Guardians and Heads of Service has already been delivered and key councillors will be trained in June. A further programme is being developed to provide relevant training for all other employees. This will be designed and delivered according to requirement of service areas.

4.8 Business Continuity

Clear linkages have been identified between the Council's Business Continuity Programme (BCP) and the IG Programme in respect of commonalities relating to information assets, business processes and business function dependencies/risks. The information already collated under the BCP will be used to pre-populate the templates needed for IG records to prevent duplication of effort and ensure consistency.

5 STATUS OF ORGANISATIONAL COMPLIANCE

Information Governance Toolkit

The Council carries out self-assessments of its compliance through completion of the Information Governance Statement of Compliance (IGSoC) so that it be assured of reaching required standards. Scoring is from 0 to 3, with 0 indicating no measures or plans in place and 3 which is good. Level 2 is satisfactory and the minimum level for processing patient identifiable NHS health data.

Assessment is against the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Secondary Uses Assurance
- Corporate Information Assurance.

The Council completed and submitted its annual return for 2015/2016 in March and is awaiting the results. Under the self-assessment criteria, three areas were assessed at level 3:

REF NO.	ITEM
13-376	Business continuity plans are up to date and tested for all critical information assets (e.g. data processing facilities, communications services and data) and service - specific measures are in place
13-378	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
13-379	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely

No requirements have been scored at less than level 2.However, attainment of this is based on implementation of the IG Improvement plan in the following areas:

REF NO.	ITEM	*PROPOSED COMPLETION DATE*
13-146	Contracts have adequate information Governance clauses. Survey required and modification of any inadequate contracts.	*December 2016*
13-148	Delivery of IG training to all staff and inclusion in induction processes for new starters (including contractors).	*December 2016*
13-252	Additional service specific data protection and data sharing training in required areas	*December 2016*

13-254	Provision of privacy notices and mechanisms for obtaining and recording consent for all services where personal data is collected.	*March 2017*
13-255	Review of data sharing agreements and creation of agreements.	*September 2016*
13-256	Structured process for including IG requirements in system/process changes. Implementation of the Asset Change Notification procedure/ PIAs and system security policies.	*September 2016*
13-372	Formal process for information security risk assessment of information assets. Completion of Information asset register. Risk reviews by IAOs. Implementation of an asset change notification process.	*September 2016*
13-375	Data flow mapping. (*Links with 13-255*).	*September 2016*
13-382	Information asset register completion.	*September 2016*
13-383	Central oversight and review regarding psuedonymisation of personal information used for secondary purposes.	*March 2017*
13-443	Central oversight and review regarding the data quality of care records.	*March 2017*
13-444	Development of a strategy to improve tracking of paper records, specifically relating to Care	*May 2017*

The current improvement plan fully aligns the Council's IG arrangements with the toolkit with the exception of items 13-383 and13-443 above. The toolkit also requires each instance of home/remote working to be approved. The council's policy allows all employees to work in this way, but it does not a present a problem of non-compliance because laptops are designed to operate securely in this environment. The policy also includes instruction relating to not allowing screens to be viewed when in a public space and not to store data on the actual laptop itself.

The Council is also accredited under the Public Services Network Code of Compliance (PSN CoCo), which is based on ISO27001 requirements.

In 2014/2015, the Council scored 69% and was assessed at level 2 compliance (satisfactory), once improvement actions were provided for evidence. Assessment for 2015/2016 remains at level 2, with a score of 70%. The implementation of further improvements during 2016/2017 aim to increase the score by at least 10%.

Overall levels of compliance for all Local Authorities that are subject to the IGSoC are published on the IG toolkit site.

6 SERIOUS INCIDENT REPORT INVESTIGATIONS

There have been no ICO reportable data protection incidents for the period 1st April 2015 to 31st March 2016 and the Council has not received any enforcement actions or monetary penalties. The table below shows the data breaches that have occurred in that period:

DATE	NO. OF INCIDENTS	TYPE	NO. REPORTABLE TO ICO
2015	1	Cyber incident	0
2015	3	Loss / theft	0
2015	11	Inappropriate disclosure - paper	0
2015	12	Inappropriate disclosure - digital	0
2016	16	Loss / theft	0
2016	6	Inappropriate disclosure - paper	0
2016	14	Inappropriate disclosure - digital	0
2015/2016 TOTAL	**63**		0

7 REQUESTS UNDER FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS

The table below shows the number of FOI and EIR requests received by the Council for 2015/2016

FOI and EIR requests 2015/16	Requests	Late response	Full response	Partial response	Refused	Reviews	ICO complaints
Apr	127	20	95	17	1	0	2
May	114	20	79	19	0	2	1
Jun	129	21	97	15	3	2	0
Jul	122	13	93	10	6	4	0
Aug	107	12	77	15	6	3	0
Sep	106	2	84	14	2	2	1
Oct	126	9	107	14	1	1	0
Nov	117	1	91	16	0	3	1
Dec	93	6	71	8	2	2	0
Jan	127	2	103	10	2	5	2
Feb	149	2	113	25	5	1	0
Mar	143	11*	100*	15*	12*	4	1
Total	**1460**	**108**	**1010**	**163**	**28**	**29**	**8**

NOTE:

- * denotes provisional figures as at 25 April 2016
- Includes open requests received in March which are not yet over the 20 working days deadline.
- 40 working days are allowed for reviews, there are still some open which again may not make the deadline.

Of the 1,460 requests received, 7.4% were responded to outside of the 20 working day deadline, 12.6% had exemptions applied to the request, 1.9% were refused a response, 2% of responses had to be subject to review as the requesters were not happy with the initial response and 0.5% were referred as a complaint to the ICO. A further breakdown is provided below:

7.1 Exemptions and Exceptions

FOI exemptions applied	
8. invalid format	2
12. Exemption where cost of compliance exceeds appropriate limit	64
14. Vexatious or repeated requests	3
21. Information accessible to applicant by other means	33
22. Information intended for future publication	7
30. Investigations and proceedings conducted by public authorities	1
31. Law enforcement	5
32. Court records	2
36. Prejudice to effective conduct of public affairs	1

FOI exemptions applied (continued)	
38. Health and safety	2
40(1). Personal information of applicant	2
40(2). Personal information of another person	50
40(5). Personal information neither confirm nor deny	1
41. Information provided in confidence	3
42. Legal privileged	1
43. Commercial interests	7
TOTAL FOI EXEMPTIONS	**184**

EIR exceptions applied	
6(1)(b) the information is already publicly available and easily accessible to the applicant in another form or format	9
12(3) the information requested includes personal data of which the applicant is not the data subject, the personal data shall not be disclosed otherwise than in accordance with regulation 13.	44
12(4)(b) the request for information is manifestly unreasonable;	9
12(4)(c) the request for information is formulated in too general a manner and the public authority has complied with regulation 9;	1
12(4)(d) the request relates to material which is still in the course of completion, to unfinished documents or to incomplete data; or	1
12(5)(b)the course of justice, the ability of a person to receive a fair trial or the ability of a public authority to conduct an inquiry of a criminal or disciplinary nature;	4
12(5)(d) the confidentiality of the proceedings of that or any other public authority where such confidentiality is provided by law;	7
12(5)(e)the confidentiality of commercial or industrial information where such confidentiality is provided by law to protect a legitimate economic interest	15
12(5)(f) the interests of the person who provided the information	9
TOTAL EIR EXEMPTIONS	**99**

7.2 Reviews and ICO Complaints

Result of Reviews	
Add exemption	2
Disclose all	2
Disclose part	2
Failed to comply with time limit	2
Maintain position	11
Supply more information	8
Not yet completed	2
TOTAL	**29**

Result of FOI/EIR complaints to ICO	
Complaint upheld	5
Complaint not upheld	1
Withdrawn	1
Pending	1
TOTAL	**8**

8 DATA PROTECTION / SUBJECT ACCESS REQUESTS

The table below shows the number of Subject Access Requests received by the Council for 2015/2016.

	Total	Late Responses
Subject Access Requests	154	73*
Police/CPA/LA protocol	137	n/a
Other lawful disclosure	24	n/a
ICO complaints	5	

*provisional figures as at 25 April.

The current structure of the team (as shown in section 2.3) has been reviewed to provide adequate future resource to significantly reduce the number of late responses.

A further review will be carried out on existing processes for dealing with FOIs/EIRs and SARs to look at how and if this can be simplified. It will also take into account the requirements under the new EU Data protection regulations, which come into effect in May 2018.

9 RISK MANAGEMENT & ASSURANCE

The Council currently has little or no activity relating to the production and review of information flow mapping, information asset registers and information risk assessments, although risks associated with business continuity have been identified and reviewed as part of the recent Business Continuity Planning Programme The risk is being mitigated by the work that the new Information Governance Team will lead on, together with the IG training that has been undertaken by Corporate and Associate Directors and Heads of Service includes specific detail relating to the three areas mentioned above.

The Council also has an overarching risk management strategy, which refers to but is not specifically aimed at the management of information risks (Risk Management Strategy). An Information Risk Policy will be developed as part of the IG improvement programme and the SIRO will have overall responsibility for the implementation of this. Asset Owners will be responsible for the production of quarterly reports to the Information Governance Board, detailing high risk areas (including mitigating actions) and the number and type of serious incidents within the reporting period.

Information risks will be included in service areas' risk registers and, if appropriate, within the Corporate Risk Register. Reporting will be in accordance with IG governance and will also be included in the quarterly reports presented to the Strategic Performance & Risk Management Board.

A significant area of concern relates to the sharing of council premises with partners that is identified as a significant risk. The Council's strategy has included the creation of three office hubs as well as Health and Wellbeing Centres, in which public service partners (such as Police, Fire and Citizens Advice) are present. This approach is in accordance with the Cabinet Offices' One Public Estate programme (OPE), which actively encourages public sector organisations to co-locate, to demonstrate efficiencies and to deliver more integrated and customer focused services. The Council has a very active part in this programme having already received a grant of £350k from phase 3 and is looking to submit a further bid in round 4. The ICO concern appears to be at odds with the council's strategic objectives and that of central government. The issue is being raised with the ICO, Cabinet Office, LGA and GPU to actively seek guidance on the inconsistency of information that has been received.

.

10 EQUALITIES

It is anticipated that there will be no equality implications associated with this report

11 FINANCE

There are no costs attached to any of the recommendations contained in this report

Dr Carlton Brand, Corporate Director and SIRO

Date: **16 May 2016**

Report Author:

Liz Creedy, Head of Partnerships and Governance

Email**:** liz.creedy@wiltshire.gov.uk

Tel: 01225 713086