Wiltshire Council
Where everybody matters

INFORMATION GOVERNANCE
SENIOR INFORMATION RISK OWNER ANNUAL REPORT
APRIL 2016 – MARCH 2017

1. PURPOSE

This report provides an overview of current Information Governance status 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 2016/2017 and to outline the next steps for 2017/2018.

2. BACKGROUND

An information governance improvement programme was developed to address the recommendations in the ICO's report issued in March 2015. The programme has been supported by the programme office under the overall direction of Dr Carlton Brand as the Senior Information Risk Owner (SIRO).

Significant progress has been made in the areas for improvement identified in the ICO's report, with 93% of the recommendations / actions now completed. An updated action plan was sent to the Information Commissioner's Office in March 2016 and notice was received in April 2016 that the audit engagement is now complete. Actions have been identified and are in accordance with the requirements of the Information Governance Toolkit.

The current status of the programme is as follows:

Scope area	Number of recommendations in each scope area from the original audit report	Number of actions complete, partially complete and not implemented. Last report 15/16	Number of actions complete, partially complete and not implemented. Current Status
Records Management	31	6 Completed 25 in progress	30 Completed 1 in progress
Subject Access Requests	27	16 Completed 11in progress	27 Completed
Data Sharing	16	0 Completed 16 in progress	12 Completed 4 in progress
TOTAL **TOTAL COMPLETE** **TOTAL IN PROGRESS**	**74** **69 (93%)** **5 (7%)**		

2.1 Physical Records Storage

Records that were held across the County in a number of storage depots were purged and catalogued as per the requirement of moving them to the new storage facility administered by Iron Mountain. The contract with Iron Mountain was signed on 31st August 2016. There were a total of 33,245 boxes relocated and the IG team co-ordinated this project to ensure that the deadline of March 2017 was achieved. As a result, we were able to release a storage facility in Devizes back to the Landlord, together with space across the County which has been utilised by the Council's Facilities Management.

An action 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. This will include working with service teams to ensure they update the retention schedule and to encourage them to catalogue their boxes. By doing this both the team and the organisation have a clearer understanding of the information they hold. It is important to do this for two reasons. Firstly, the less we store, the less space we take up and the less requests we have to make to the external provider.

Secondly we must have a better understanding of what information we hold. To become an organisation which promotes an open and transparent approach to the way it takes decisions and conducts business, we must be robust about what information we actually need. This applies to both the physical records as well as the digital records we keep.

2.2 Information Governance Policies

A comprehensive suite of information governance policies has now been written and approved by the IG Board and 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 and Environmental Information Regulations
- Records Management
- Information Security
- Mobile Working
- Network Security
- Information Asset Change
- IG Communication and Engagement Strategy
- IG Training Strategy

2.4 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, together with the need to discharge these diligently as an integral part of their day to day work.

If this cultural change is to take place it is key that Corporate and Associate Directors, Caldicott Guardians and Heads of Service engage with and play a key role in ensuring that staff understand their responsibility for good Information Governance.

The IG Communication plan, which was taken to the IG Board in early 2017 and approved, outlines the ways in which the IG team will engage across the organisation. This will range from newsletters to attending team meetings, to offering targeted training and having a workspace on GROW which people can access to find out more about Information Governance

3. ASSURANCE FRAMEWORK

Information Governance (IG) Board and Information Governance Assurance Group (IGAS)

The above two groups have been established and terms of reference drawn up to ensure robust monitoring of the effectiveness of the Council's information governance arrangements. The IG Board is currently chaired by the SIRO (Dr Carlton Brand) and includes the Caldicott Guardians for Childrens' Services, Adult Care and Public Health, the Monitoring Officer, Associate Director for Corporate Function, Procurement and Programme Office (Deputy SIRO) and the Head of Partnerships and Governance (Deputy SIRO). It is responsible for the overall monitoring and decision making relating to IG. The IGAS includes the new IG leads for data protection; FOI; information security and records management. The IGAS is responsible for reviewing practices across the council to ensure they are relevant and fit for purpose.

As the original purpose for the IG Board was to ensure the recommendations from the ICO Audit were actioned, a review of both the Terms of Reference and purpose will be discussed to decide the future role of the board and to outline the IG roadmap going forward.

4. STATUS OF ORGANISATIONAL COMPLIANCE

Information Governance Toolkit

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 Council carries out self-assessments of its compliance through completion of the Information Governance Statement of Compliance (IGSoC) so that it can 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 2016/2017 in March and is awaiting the results.

These were the IG toolkit requirements we met when we self-assessed at the highest level, Level 3.

REF NO.	ITEM
13-144	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
13-145	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
13-373	There are documented information security incident / event reporting and management procedures that are accessible to all staff
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
13-380	Policy and procedures ensure that mobile computing and teleworking are secure
13-441	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience

One requirement was reduced from Level 3 to level 2. This is due to additional requirements which are only applicable when level 3 was attained in the previous year, redesign of and ICT restructuring. It is anticipated that level 3 will regained in the next submission

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	Revised Date	Comment
13-146	Contracts have adequate information Governance clauses. Survey required and modification of any inadequate contracts.	*Dec 2016*	April 2018	This action has become a core work stream in the GDPR project and has been allocated to Procurement to take forward, but this will require input from other services
13-148	Delivery of IG training to all staff and inclusion in induction processes for new starters (including contractors).	*Dec 2016*	Ongoing	HR/OD are currently in a procurement process that will provide access to a number of e-learning modules that IG will be able to use. This will also be used as the basis for the Corporate Induction Programme.
13-252	Additional service specific data protection and data sharing training in required areas	*Dec 2016*	Ongoing	A new GDPR presentation has been developed and is being delivered. The Information Risk survey will highlight further service specific training requirements
13-254	Provision of privacy notices and mechanisms for obtaining and recording consent for all services where personal data is collected.	*March 2017*	April 2018	Again this action, now falls in the requirements for GDPR. Privacy notices have been rewritten and work is in progress to expand individual notices. NHS national GDPR guidance and the new version of the IG toolkit is currently awaited to provide further direction
13-255	Review of data sharing agreements and creation of agreements.	*Sept 2016*	April 18	This has become part of the GDPR project. However, this is also an ongoing piece of work in collaboration with the Information Asset Owners (IAO's) to ensure that where information is being shared that it is done with an appropriate sharing agreement.
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.	*Sept 2016*	Ongoing	A significant part of this action has been achieved. The IG team continue to work with IAO's to ensure a clear understanding of assets and information sharing understood. Progress has not been as quick as the IG team would have liked but this is very much a task reliant on responses predominantly from Heads of Service and other priorities take over.
13-375	Data flow mapping. (*Links with 13-255*).	*Sept 2016*	April 2018	This has become part of the GDPR project. The Information risk survey will identify higher risk data flows and they will be logged as part of the GDPR requirements for Records of Processing Activity (ROPAs)

Ref No.	Item	Proposed Completion Date	Revised Date	Comment
13-382	Information asset register completion.	*Sept 2016*	Ongoing	Much is completed and now depends on the review of responses from IAO's
13-383	Central oversight and review regarding psuedonymisation of personal information used for secondary purposes.	*March 2017*	Ongoing	This is an action that is constantly rolling forward. The Caldicott Guardians have a responsibility due to the cross service sharing of NHS information. This will come through the IGASG for review.
13-443	Central oversight and review regarding the data quality of care records.	*March 2017*	Ongoing	As above

The IG improvement plan and GDPR Project fully aligns the Council's IG arrangements with the toolkit with the exception of items 13-383 and13-443 above.

5. PSN

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%. For 2016/2017, the target was 80% but due to the GDPR and the NHS National Data Guardians Review, there may be some changes to the requirements for the next version of the IG toolkit when it is published. At the time of writing this report, the final score was still awaited.

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 was one ICO reportable data protection incident for the period 1st April 2016 to 31st March 2017. The Council has not received any enforcement actions or monetary penalties for this period.

With regard to the incident reported to the ICO, the Council wrote to the Commissioner's office on 10th February providing further details, following information from West Midlands Police of suspected illegal access to one of the Council's training websites. Investigation showed that no personal details were disclosed. The ICO made some recommendations which have been incorporated into the Information Governance Programme plan.

Data Incidents

With regard to data incidents, the table below shows the data breaches that have occurred in 2016/2017.

DATE	NO. OF INCIDENTS	TYPE	NO. REPORTABLE TO ICO
2016	6	Failure to follow procedure	0
2016	15	Inappropriate Disclosure	0
2016	27	Loss or Theft	0
2016	4	Near Miss	0
2016	5	Other	0
2017	4	Inappropriate Disclosure	0
2017	8	Loss or Theft	0
2017	1	Other	0
2016/2017 TOTAL	**70**		0

Whilst there is a slight rise in data incidents from 2015/2016, it is not significant and attention should be given in particular to the reduction of incidents involving Loss or Theft. A rise to 35 for 2016/2017 from 19 in the previous year.

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

Risk Management & Assurance

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).

Priority has been given to the practical identification and detection of information risks. Information asset owners are currently completing an information risk survey in the areas of data protection compliance, IG awareness, information handling and future business changes. From the responses, potential risks will be identified by the IG team and followed up to find resolutions. Open risks will be added to the corporate risk register by the IG team or services registers by IAOs as applicable.

The IG team are working collaboratively with IT to identify a new set of metrics which will monitor potential Information security risks. The measures will be based on the National Cyber Security Centre's 10 Steps to Cyber Security but also take account of the nature of technological change (cloud computing) and the increasing mobility of devices, people and information

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 2016/2017. In comparison to last year, the total has raised slightly from 1,460 for 2015/2016.

FOI and EIR requests 2016/17	Requests	Late response	Full response	Partial response	Refused	Reviews	ICO complaints
Apr	119	14	88	19	9	3	0
May	119	15	91	19	4	2	0
Jun	111	15	86	8	12	0	0
Jul	125	23	88	4	18	4	5
Aug	130	25	102	2	8	2	0
Sep	119	22	74	5	12	2	0
Oct	134	26	98	5	8	2	0
Nov	148	8	98	8	13	3	0
Dec	110	11	76	9	11	4	0
Jan	147	14	102	11	6	2	0
Feb	128	6	88	18	4	3	0
Mar	142	9	80	16	12	2	0
Total	**1532**	**188**	**1071**	**124**	**117**	**29**	**5**

Of the total 1,532 requests received, 87.5% were responded to within the legal compliance date of 20 working days, 8% of the total requests responded to had exemptions applied to the request. Out of the 1532, 7.6% were refused a response and 8% of total responses were subject to review following a complaint from the requesters.

A further breakdown is provided below:

8.1 Exemptions and Exceptions

FOI exemptions applied	
8. invalid format	2
12. Exemption where cost of compliance exceeds appropriate limit	48
21. Information accessible to applicant by other means	49
22. Information intended for future publication	5
31. Law enforcement	7
38. Health and safety	2
40(1). Personal information of applicant	2
40(2). Personal information of another person	36
40(5). Personal information neither confirm nor deny	8
41. Information provided in confidence	2
42. Legal privileged	1
43. Commercial interests	5
TOTAL FOI EXEMPTIONS	**167**

EIR exceptions applied	
6(1)(b) the information is already publicly available and easily accessible to the applicant in another form or format	17
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.	26
12(4)(a) the authority does not hold that information when an applicant's request is received	3
12(4)(b) the request for information is manifestly unreasonable;	17
12(4)(c) the request for information is formulated in too general a manner and the public authority has complied with regulation 9;	2
12(4)(d) the request relates to material which is still in the course of completion, to unfinished documents or to incomplete data; or	6
12(4)(e) the request involves the disclosure of internal communications.	2
12(5)(a) international relations, defence, national security or public safety	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;	3
12(5)(d) the confidentiality of the proceedings of that or any other public authority where such confidentiality is provided by law;	4
12(5)(e)the confidentiality of commercial or industrial information where such confidentiality is provided by law to protect a legitimate economic interest	10
12(5)(f) the interests of the person who provided the information	9
TOTAL EIR EXEMPTIONS	**100**

8.2 Reviews and ICO Complaints

The two tables on the next page outline the number of reviews and ICO complaints that were received in this reporting year. Reviews are considered by members of the IG Team who have had no direct involvement in the original request, to ensure independence. Complaints are received from the Information Commissioner's Office.

Result of Reviews	
Disclose all	2
Maintain position	18
Supply more information	9
TOTAL	**29**

Result of FOI/EIR complaints to ICO	
Complaint upheld	4
Complaint not upheld	1
TOTAL	**5**

10. DATA PROTECTION / SUBJECT ACCESS REQUESTS

The table below shows the number of Subject Access Requests received by the Council for 2016/2017.

	Total	Late Responses
Subject Access Requests	178	32
Police/CPA/LA protocol	140	n/a
Other lawful disclosure	24	n/a
ICO complaints	6	n/a

These are the figures 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	

The structure of the team 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 consider the requirements under the new EU Data protection regulations, which come into effect in May 2018.

11. FUTURE DEVELOPMENT PLANS

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	PROPOSED DELIVERY TIMESCALE
Information Asset Register completed	September 2017
Survey to review continued paper records needs of the organisation	September 2017
New Retention Schedule	June 2017
Gap Analysis Project to establish what we must publish under FOI	December 2017
GDPR Project	April 2018

ITEM / SUBSIDIARY PROJECT	PROPOSED DELIVERY TIMESCALE
Review of risk management to include improved monitoring and reporting	December 2017
New Policy for Acceptable use	September 2017
New Policy for Sharing Personal Information	September 2017
New Classification Policy	August 2017
Revised process for reporting Data Breaches	September 2017
E-learning training	September/October 2017
Development of IG workspace on GROW	August 2017
Completion of ICO Recommendations	December 2017
Plan IG Toolkit responsibility for 17/18 assessment	March 2018

There are several 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.

12. SUMMARY AND RECOMMENDATIONS

This report highlights the achievements made by the Council within the IG programme for 2016-2017. It should be acknowledged that the IG team, who have only worked together as a team since September 2016, have worked extremely hard to ensure that they have kept up with the pace of demands of the Information Governance improvement agenda in addition to the day to day operational aspects of IG.

There has been a significant increase in information security breaches of personal information in both the national and international arena. We cannot therefore be complacent or have a casual approach with our own information governance and security processes. If our aim is to operate in a more digital environment, we must be robust in our management of sensitive information, understand who we are sharing that with, have the right processes in place to monitor the correct use and ensure our staff understand their role in keeping information safe.

The IG framework is a large and complex agenda and the IG team are front and centre in delivering that. There are significant challenges ahead, only heightened by the interest of the public following the reporting of adverse events through the media.

The priority for the Council is to inculcate a cultural change for both staff and Members in its approach to Information Governance and that it continues to develop and progress to ensure statutory compliance with current and emerging legislation.

Dr Carlton Brand, Corporate Director and SIRO

Date: 1st August 2017

Report Author:

Sarah Butler, Information Governance Manager

Email: sarah.butler@wiltshire.gov.uk Tel: 01225 718446