DORSET & WILTSHIRE FIRE AND RESCUE AUTHORITY

Item 17/40

INFORMATION GOVERNANCE FRAMEWORK ANNUAL REPORT 2016/17

Introduction

Information Governance brings together all of the requirements, standards and best practice that apply to the handling of information on all media. The framework ensures that the organisation and individuals have information that is accurate, meets legal requirements, is dealt with efficiently and is secure. It supports the Information management policy and has four fundamental aims:

- To support and promote the effective and appropriate use of information;
- To encourage responsible staff to work together, preventing duplication of effort and enabling more efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- To enable us to understand our own performance and manage improvement in a systematic and effective way.

The framework currently encompasses:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Information Sharing
- The Confidentiality Code of Practice
- Records Management
- Information Quality Assurance
- Information Security
- Information Governance Management
- Risk Management
- Data Transparency

The Services policy statement relating to Information Management has been reviewed and updated to ensure all aspects of this discipline are recorded and accountable. The intent is to demonstrate continued delivery against those commitments in the policy statement through this annual assurance report.

Grading

Excellent	*Audited legal compliance achieved, no outstanding issues, high confidence*
Good	*Procedure exists. Good confidence, no major issues or failings,*
Fair	*Some good practices in place but no procedure. key issues exist, some cause of concern, action plan in place,*
Poor	*Lack of legal compliance/no good practices in place. Failings have occurred or are likely to occur, considerable areas of concern*

This grading process is applied to each policy statement and an 'at a glance' summary is provided within the report.

Overall we have 5 statements at Good and therefore for this report the overall grading is considered to be:

Good	*Procedure exists. Good confidence, no major issues or failings.*

Outstanding Key Issues

The priority allocated to Outstanding Key Issues is as follows:

H	Within 12 months
M	Within 24 months
L	Within 36 months

All high priority issues identified in this report will start to be actioned from 1 April 2017.

Policy Statement – Summary of Overall 'Ratings'

No	Statement	Rating 2017	Rating 2018
1	Maintain security of our information in line with HMG Security Policy Framework and relevant Code of Connections	**Good**	
2	Compliance with the Data Protection Act	**Excellent**	
3	Compliance with the Freedom of Information Act and Environmental Information Regulations	**Excellent**	
4	Compliance with the Regulation of Investigatory Powers Act	**Good**	
5	Promote good information management practices, taking advantage of new technologies where possible to encourage efficient and compliant systems of work	**Fair**	

2016/17 Statement of assurance		
Subject	(1) **Maintain the security of Service information, protecting its confidentiality, integrity and availability in compliance with the HMG Security Policy Framework.** We need to protect sensitive information from unauthorised disclosure, safeguard the accuracy and completeness of information and software and ensure that information and vital ICT services are available when required. Robust systems and processes will mean that we reduce the risk of legal exposure through a security breach, and are better placed to encourage the secure exchange of data with our partners, which will allow us to improve prevention and response to vulnerable groups.	
Officer	Vikki Shearing	
Date	June 2017	
Overall judgement	**Excellent**	*Audited legal compliance achieved, no outstanding issues, high confidence*
	Good	*Procedure exists. Good confidence, no major issues or failings,*
	Fair	*Some good practices in place but no procedure. key issues exist,* *some cause of concern, action plan in place,*
	Poor	*Lack of legal compliance/no good practices in place. Failings have* *occurred or are likely to occur, considerable areas of concern*

What are we assuring?

1. Effective and timely monitoring of security incidents via the reporting process and monitoring tools. (KPI)
2. Completion of annual IT health check and confirmation that corrective actions are taken and risks reduced
3. Effectiveness of change control process
4. DWFRA and SLT understanding of the information risk - SIRO, IAO, Information Asset Register, BIA, ICT and IM relationship
5. Progress against the baseline control set (ISO 27001)
6. Effective management of risks/actions and promotion of good practice through the Information Governance Group and considered as part of the project management, business change and procurement process.

7. Completion of regular staff awareness - staff understanding and compliance with their responsibilities ensuring a culture of valuing information as an asset
8. Effective technical controls are in place preventing unauthorised disclosure of information and reducing the risk of vulnerabilities
9. Effective use of Governments classification scheme
10. Information risk is considered as part of the project management, business change and procurement process for all third parties
11. Information Asset Owners understand their responsibilities and are managing systems and risk
12. Effective security clearance process
13. Corporate security policy in place
14. Effective business continuity plans in place

Basis of judgement

Since 2016 work has been focused on alignment of practices for information governance and security. This area was the subject of an internal audit which provided substantial assurance for the Authority with minor improvement areas which have been completed.

1. The Information Security Incident process is well established and has been communicated to staff. Incidents are monitored quarterly at the Information Governance Group. In the last year, 14 incidents were reported by staff. These related to lost mobile phones (5), virus attacks (4), and minor misuses of data that had no malicious intent (5). In 11 of these incidents, there was no compromise to our data, 1 had the potential to compromise and 2 were minor compromises. Our internal processes and technical solutions enabled us to reduce damage and mitigate risks effectively.
2. An annual IT Health Check was carried out in 16/17 and the corrective action plan monitored on a weekly basis to ensure all high and medium risks were resolved within agreed timescales. Given the work of bringing together 2 ICT networks and the alignment of many IT processes and systems, this check identified very few high risks which we were not already aware of and programming in as part of our transition work. The IT Health Check for 2017 is programmed in for May.
3. The Change control process is under a period of consultation and will be published in the next 4-6 weeks.
4. The SIRO attends the quarterly Information Governance Group and is kept informed of key issues and risks in relation to information security which are fed back to SLT where necessary, via the risk management process in sycle.
5. The Service is in the process of aligning its Baseline Control Sets as a result of combination to maintain compliance with the requirements of the ISO 27001.
6. Information Risk Management is corporately led by the Information Management team and supported by clear roles and responsibilities which include Information Asset owners, the Information Governance Group and IT Security Officer. These are outlined in procedures.
7. Completion of the online Security Awareness training is monitored regularly, to ensure that refreshers are completed bi-annually and that new starters complete the course as part of the induction process. This process will be fully automated during 17/18, the course will be reviewed during 17/18 to reflect the new GDPR. Through internal communications, lessons learnt from security breaches and subject access requests, as well as champions in the Information Asset

owners, staff awareness of information security is good. Concerns and risks are being raised through project teams, information asset owners and at department meetings.

8. The Information Security Officer attends the Information Governance Group and works closely with the Information Manager to ensure technical controls are in place which are relevant to risk.
9. The information handling procedure has been updated to reflect the new approach under the Government's Classification Scheme. Clear handling instructions for information assets is included in the procedure and this has been delivered to all department meetings, with a focus on sensitive information. The on line training also reflects the new approach.
10. All new projects have to undergo a security assessment in the early stages of the project development. This enables relevant controls to be implemented to effectively mitigate risks during the planning phase. Security is also included in the procurement process to ensure third party systems and services meet security requirements.
11. Information Asset Owners for the new Service have been identified and trained. IAO's have provided annual assurance for 2016/17 that the security of their information is being managed appropriately and there is quality control in place to ensure the accuracy of information they process. Asset Owners are also involved in developing the Information Asset Register which will be monitored quarterly.
12. BPSS is carried out on all new staff as part of the recruitment process. There is a programme to ensure this standard is applied across the board to existing staff. Higher levels of clearance are required for specific roles and this is also picked up during the preparation for recruitment and promotion.
13. The Corporate Information Security Policy is in place.
14. Business continuity considerations have been built into all security procedures and an up to date departmental plan exists to ensure the management of our information in these circumstances.

Outstanding key issues	Priority			Improvement required	Lead
A brief summary of the outstanding issues	**H**	**M**	**L**	What is being done or is proposed to address the outstanding issue	Who is leading
Two security management procedures still exist and need to be aligned now that networks are aligned.				Complete the alignment of the security management procedure	L Smith
Two baseline assessments still exist. These need to be aligned now that single technical controls, procedures, systems and processes are in place to ensure gaps and risks are mitigated				Review and align baseline control sets for ISO compliance	L Smith

BPSS not applied to all DWFRS staff				Deliver a programme to align all existing staff to BPSS	S Price

2016/17 Statement of assurance

Subject	**(2) Compliance with the Data Protection Act.** The Service is registered as a Data Controller under the Act and as such must comply with the 8 principles relating to the processing of personal data. This includes, ensuring we have a legal right to process the data, or consent to do so, we are only collecting what we need and for retaining it for no longer than necessary. We are keeping the information up to date, accurate and ensuring it's security. We are processing all personal data in line with Data Subject Rights.	
Officer	Vikki Shearing	
Date	June 2017	
Overall judgement	**Excellent**	*Audited legal compliance achieved, no outstanding issues, high confidence*
	Good	*Procedure exists. Good confidence, no major issues or failings,*
	Fair	*Some good practices in place but no procedure. key issues exist,* *some cause of concern, action plan in place,*
	Poor	*Lack of legal compliance/no good practices in place. Failings have* *occurred or are likely to occur, considerable areas of concern*

What are we assuring?

15. Adequate and relevant process in place for handling Subject Access Requests which allows us to meet our legal requirements.
16. Adequate and relevant process in place compliant with ICO guidelines for disclosure and enforcement regime
17. Effective retention procedures in place
18. Registration with the Information Commissioner is accurate and up to date
19. Privacy Impact Assessments are in place for high risk areas of processing personal data
20. Staff understanding and undertaking their responsibilities
21. Effective data sharing agreements and MOU's are in place
22. Relevant and effective use of secure email for sharing personal data
23. Staff have confidence in the way in which we handle their personal data

Basis of judgement

15. Formal Subject Access requests are managed centrally to ensure compliance with the 40-day deadline. There is a procedure in place which details responsibilities and awareness is included

at induction and through the protecting information on line training course. Subject Access Requests are monitored quarterly and in the last year all of the 13 we received were handled within the 40-day deadline. Providing staff access to their information is a key part of the work of HR and for that reason we are working closely with the teams to strengthen their understanding and therefore continue to ensure our compliance in this area.

16. An effective procedure for Managing Personal Information is in place. The Service is kept abreast of changes in legislation and updates as necessary via the National FRS Forum and ICO. The team are currently receiving training in relation to the new data protection regulations which come into force in May 2018. This will inform the Services action plan for compliance.
17. Retention guidelines are in place for information held by the Service. This is now reflected in the Information Asset Register and will now start to form part of the review of our Archive process.
18. The new Authority's registration with the ICO is current.
19. A significant amount of work has been achieved in the last year to raise awareness of Privacy Impact Assessments, to ensure these start to become standard practice for all new and changes to existing systems, process and procedures. This approach has meant that managers recognise the importance of privacy and the actions they need to take to ensure the security of our information. Privacy considerations are prompted in procedure checklists during development of the new procedures and project creation in the performance management system. The requirement has been incorporated into the Data protection procedure.
20. DPA awareness is included at induction. Online DPA training is completed by all staff and a full refresher course is completed bi-annually. This, combined with a low number of security incidents demonstrates that staff are clear on their responsibilities. Specific training is also provided to teams handling sensitive personal data on a regular basis. The team are well regarded across the Service and staff know where to access advice and support if they have concerns.
21. Data sharing procedure are in place. Information Asset Owners are aware of their responsibilities to protect and disclose information as appropriate. The Service are signatories to the data sharing protocols (Single View and DISC) that exist in the two counties. The Service is a key partner in the implementation of these, promoting these across teams who work with external partners.
22. Egress is used to exchange data securely with third sector and this is working well with partners of SAIL.
23. Levels of staff confidence in the way that the Service manages their personal data was not included in the recent staff survey and we will ensure this is covered in the survey during 2018.

Outstanding key issues	Priority			Improvement required	Lead
A brief summary of the outstanding issues	**H**	**M**	**L**	What is being done or is proposed to address the outstanding issue	Who is leading
None					

2016/17 Statement of assurance		
Subject	(3) Legal compliance with the **Freedom of Information Act**, ensuring information is accessible in the spirit of openness and transparency	
Officer	Vikki Shearing	
Date	June 2017	
Overall judgement	**Excellent**	*Audited legal compliance achieved, no outstanding issues, high confidence*
	Good	*Procedure exists. Good confidence, no major issues or failings,*
	Fair	*Some good practices in place but no procedure. key issues exist,* *some cause of concern, action plan in place,*
	Poor	*Lack of legal compliance/no good practices in place. Failings have* *occurred or are likely to occur, considerable areas of concern*

What are we assuring?

24. Publication Scheme is maintained to reflect new and changing information access requirements. The Information available through the website reflects the demands of the public and legal requirements and is helping with the wider community engagement and consultation agenda
25. Procedure up to date reflecting legal requirements and good practice
26. Effective process in place for handling – logging and responding to Freedom of Information Requests and Environmental Information requests and ensuring these are dealt with in line with legal requirements
27. Information assets are made publically available if necessary in compliance with the Transparency code of practice
28. Staff understand FOI legislation

Basis of judgement

24. The Publication scheme is available on our website and this reflects the Code of Date Transparency.
25. The Access to Information procedure was aligned for the new Service on 1 April 2016 and is up to date and relevant.
26. In the last year, the service has received 126 requests for information under the FOIA and only 1 of those exceeded the 20 working day deadline, by a day. This is a really positive position, despite the complexities since combination, where large amounts of data are still being held in two separate legacy systems, often in different format, managed by different staff and recorded in different ways.
27. IAOs provide an annual review of their assets which includes recognition of areas where information can be made available publically, via our website. The Service is compliant with the Governments Code of Transparency and makes information available under this code, aligning it on the Service website with the publication scheme.
28. All FOI's reach the team and there has been no cause for concern in this area.

Outstanding key issues	Priority			Improvement required	Lead
A brief summary of the outstanding issues	**H**	**M**	**L**	What is being done or is proposed to address the outstanding issue	Who is leading
None					

2016/17 Statement of assurance		
Subject	(4) Legal compliance with the **Regulation of Investigatory Powers Act** which provides the Authority with powers to access communications data or carry out covert surveillance for specific purposes relating to public safety and the prevention of crime	
Officer	Vikki Shearing	
Date	June 2017	
Overall judgement	**Excellent**	*Audited legal compliance achieved, no outstanding issues, high confidence*
	Good	*Procedure exists. Good confidence, no major issues or failings,*
	Fair	*Some good practices in place but no procedure. key issues exist,* *some cause of concern, action plan in place,*
	Poor	*Lack of legal compliance/no good practices in place. Failings have* *occurred or are likely to occur, considerable areas of concern*

What are we assuring?

29. Effective authorisation process in place for all elements of the legislation – intercepting communications data, acquiring communications data, conducting covert surveillance, the use of covert human intelligence sources and access to electronic data protected by passwords and encryption
30. Completion of annual reports to Interception of Communications Commissioners Office
31. Staff understand their responsibilities under the Act
32. Procedure is up to date reflecting legal requirements and good practice

Basis of judgement

29. The Authority's procedure has been validated by external inspectors from the Office of Surveillance Commissioner as effective in compliance with the legislation
30. The Annual reports for both the OSC and the IOCCO are completed – there has been no use of our Powers under RIPA.

31. Relevant authorising staff are aware of their responsibilities and additional refresher training is planned for 17/18 following any amendments in line with the changes in legislation
32. The RIPA procedure has been reviewed to reflect the recommendation made in both external audits conducted from previous Services and the aligned procedure has been validated by external auditors. A further review will take place this year to ensure compliance with the change in legislation when it comes into force.

Outstanding key issues	Priority			Improvement required	Lead
A brief summary of the outstanding issues	**H**	**M**	**L**	What is being done or is proposed to address the outstanding issue	Who is leading
RIPA training to reflect changes in legislation				Provide refresher training to all staff with responsibilities for RIPA, including CFO and ensure CHIS is also covered	L Smith
Revised legislation could impact existing practices				Review existing procedure and update to incorporate any changes as a result of the amended regulations.	L Smith

2016/17 Statement of assurance

Subject	(5) Promote **good records management practices**, taking advantage of new technologies where possible to enable us to effectively store, access and destroy our information as required. This will promote legal compliance with DPA and FOI, support effective decision making and enable us to report our performance accurately.	
Officer	Vikki Shearing	
Date	June 2017	
Overall judgement	**Excellent**	*Audited legal compliance achieved, no outstanding issues, high confidence*
	Good	*Procedure exists. Good confidence, no major issues or failings,*
	Fair	*Some good practices in place but no procedure. key issues exist,* *some cause of concern, action plan in place,*
	Poor	*Lack of legal compliance/no good practices in place. Failings have*

		occurred or are likely to occur, considerable areas of concern

What are we assuring?

33. Effective use of technology to promote collaborative working across departments and information dissemination service wide
34. Policy and structure in place for good records management
35. Compliance with Corporate Retention Schedule and that the guidelines are maintained
36. Effective management of Service Archives

Basis of judgement

33. Since combination, teams have been using a cloud storage system (in addition to file shares) to collaborate and share documents. As part of the smarter working programme, options for improved collaboration has been considered, to help address the challenges of disparate teams in remote locations. In line with the roll out for office 365, use of SharePoint for document storage, version control and access control will be implemented service wide. The solution will also provide for an effective two way communications platform so that there is one place for all staff to go, to work, connect to others and share information. This will maximise the use of video and teleconferencing.
34. There are no specific records management procedures in place, but staff expectations are covered in DPA, FOI, Security, Information Handling and Retention procedures. Guidance will be provided for staff as office 365 is implemented in the use of SharePoint for document management.
35. The Retention schedule is being incorporated into the Information Asset register and filing structures will incorporate retention within SharePoint. IAOs provide annual assurance that retention guidelines for their assets are being maintained.
36. A database provides an accurate register of archives and review dates, allowing an annual process for review/destruction and the ability to search for files stored as paper records.

Outstanding key issues	Priority			Improvement required	Lead
A brief summary of the outstanding issues	**H**	**M**	**L**	What is being done or is proposed to address the outstanding issue	Who is leading
Retention procedures not aligned				Review procedure and update guidelines in consultation with Information Asset Owners	L Smith
The need to introduce effective document storage, collaboration				Consider options for delivering and effective document management solution for the	V Shearing

and access to information remotely to support staff working across disparate teams, and remotely.				new Service which is in line with office 365	