Purpose: Noted

Date **July 2018**

Title **Information Governance**

Report of Chief Officer

1 Audit objectives

1.1 This review has sought to assess the effectiveness of controls in place focusing on those designed to mitigate risk in achieving the following key objectives:

- policies and procedures for information management are defined documented, maintained and adhered to;
- training and awareness for information management is comprehensive and periodically conducted for all new and existing staff;
- Freedom of Information and Subject Access Requests (SARs) are dealt with in line with legislative requirements;
- data handling, storage, processing and destruction is in line with the 8 Data Protection principles;
- data sharing protocols have been established and are adhered to by staff to ensure that data is shared appropriately with other organisations;
- data privacy notices are published at collection and where appropriate, consent is recorded;
- privacy impact assessments are undertaken when changes are made to systems, policies and procedures;
- appropriate plans are in place and are monitored to support HFRS in being prepared for the implementation of the requirements of new data protection legislation (GDPR) taking effect from May 2018.

2 Audit opinion

2.1 The overall opinion of this review based on the audit evidence obtained, is that **limited assurance** can be placed on the effectiveness of the framework of risk management, control and governance designed to support the achievement of management objectives.

3 Executive summary

3.1 There are a number of information management related policies and procedures in place in Hampshire Fire and Rescue Service (HFRS), covering the key areas of information security and handling. We noted that several documents had not been reviewed for some time, however we were informed that HFRS are in the process of carrying out a policy review process to streamline the number of policies and procedures prior to transferring documents to Sharepoint. There were also some housekeeping issues with document control records such as version number, review dates and record of changes made.

3.2 We were informed that HFRS does not currently provide Data Protection training to all staff. Although we understand that all operational and support staff across HFRS received training three years ago, there has been no follow up to this, and new staff do not receive Data Protection training as part of their induction. However we confirmed that staff dealing with sensitive data in a safeguarding role do receive annual Data Protection training as part of that role. ICO guidance is that all staff should be trained, and that this should be refreshed annually.

3.3 HFRS have procedures in place for handling Freedom of Information (FOI) requests. Testing of FOI requests confirmed that they were being handled in line with procedures, except for completed requests being published on the HFRS website. A small percentage of requests were completed outside the 20 day limit (5.7% between April and November 2017). We tested 4 overdue requests and established that for 2 of these departments had not been reminded of the need to provide information in a timely manner. There is also no training on FOI given to staff, although the staff dealing with FOI requests have been trained.

3.4 The complaints information published on the HFRS website is incomplete, as it does not inform the complainant that they will receive a response within 20 days, or that they have a right to contact the Information Commissioner's Office if they are not satisfied with the HFRS response.

For four of the 15 FOI requests tested, we were unable to confirm that the requester had been notified of the complaints procedure as required, because some documentation was missing; we understand that this documentation was lost because of IT problems.

3.5 Procedures are in place for Subject Access Requests (SARs), and we found that these are being complied with.

3.6 At the time of the audit there was no information asset register in place, therefore HFRS could not evidence what data is held, where it is held, how it is processed and with whom it is shared. A record of data held is one of the key requirements of the GDPR, which will be effective from 25th May 2018. Discussions with the Performance Review Manager in

March 2018 indicated that the new Data Protection Officer had begun this task, however it was anticipated that it would take time to complete.

3.7 Access controls are in place for IT systems, and we found that starters and leavers accounts are assigned and deleted appropriately. There is also good physical security, with access to sites restricted. Virus protection, back up procedures and a firewall are all in place. Redundant hardware is securely disposed of by a contractor, however we noted that there were some discrepancies between the IT asset register and the records of disposal issued by the contractor.

3.8 Although there is a data incident and breach procedure in place, testing highlighted that this is not being complied with. The log of data incidents/breaches contained little information, and there was no documentation held in SharePoint to evidence the process carried out for six of the ten data incidents/breaches logged. This is a key requirement of the GDPR.

3.9 There is limited personal data sharing carried out by HFRS, with data being shared with the Multi Agency Safeguarding Hub (MASH) through a data sharing agreement drawn up by HCC. Generic Data Privacy Notices are in place, and these are in the process of being reviewed to ensure compliance with the GDPR.

3.10 Privacy impact assessments are included as part of the Project Lifecycle to ensure that they are completed in a timely manner. However, our review of the documentation for the Drones project highlighted that although a People Impact Assessment had been completed detailing equalities impacts, there was no Data Protection Impact Assessment completed. This will be a requirement of the GDPR.

3.11 Due to some of the issues highlighted above, such as the lack of general Data Protection training, absence of a record of the data held by the organisation, non-compliance with data breach procedures, and the lack of completion of Privacy Impact Assessments, there is a risk that HFRS will not be compliant with the GDPR when it comes into effect on 25th May 2018.

4 Action plans

4.1 The action plans detailed within this report provides:

- Observations where internal audit considered either controls or compliance to be insufficient to mitigate risk to the achievement of management objectives;
- The actions management propose to undertake to bring the risks within acceptable parameters; and
- Internal audit's assessment as to whether management's

actions achieve an acceptable level of risk exposure.

Action plan 1 - Information Asset Register				
Objective	Data handling, storage, processing and destruction is in line with Data Protection principles.			
Observation	We were informed by the Performance Review Manager and the Information Security Assurance Manager at the start of the audit in November 2017 that HFRS did not have an information asset register in place. At this time, blank Register of Personal Data Processing Forms (F11-1-11) had been emailed to all known data owners with the request that they be completed and returned to IT. However, further discussions with the Performance Review Manager and the Information Security Assurance Manager in February 2018 highlighted that the information asset register was still not in place. As part of the process towards GDPR compliance, every organisation needs to know what data it holds, where it came from and who it is shared with. An information asset register would keep all these details in one place. Without an information asset register in place, there is a risk that HFRS will not meet the requirements of the GDPR by 25th May 2018.			
Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
1.1	Information Asset register to be fully populated and embedded across Service in all daily working practices	H	Data Protection Officer	March 2019
Auditor's assessment of management response:				

Action plan 2 - GDPR implementation				
Objective	Appropriate plans are in place and are monitored to support HFRS in being prepared for the implementation of the requirements of new data protection legislation (GDPR) taking effect from May 2018.			
Observation	HFRS has an action plan that sets out the various actions required to enable an organisation to be compliant with the GDPR by the deadline of 25th May. This sets out a schedule of actions from February 2017 to April 2018. Discussions with the Performance Review Manager and observations during the course of the audit confirmed that although some action has been taken, this is not in line with timescales as advised by the plan. For example, the plan suggests that an information audit should have been completed by March 2017 and as at March 2018 this is currently underway at HFRS. We were advised by the Performance Review Manager that the information audit will be documented in an information asset register following meetings with Heads of Service, and this work will take approximately two months to complete. However, much of the work to comply with the GDPR will be informed by what data is collected, processed and held by the organisation, including Privacy Notices, the need to obtain consent, ensuring that contracts are in place with organisation with whom data is shared and that these are GDPR compliant. There is therefore a risk that HFRS will not be compliant with the GDPR when this becomes law in May 2018.			
Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
2.1	Update plan with appropriate time scales	M	Data Protection Officer	July 2018
Auditor's assessment of management response:				

Action plan 3 - Information management policies and procedures				
Objective	Policies and procedures for information management are defined documented, maintained and adhered to.			
Observation	Review of 18 policies and procedures relating to information management highlighted the following issues: • 14 were not dated to show when they had been drawn up • five documents did not have a review date recorded, with the remaining 13 having review dates between June 2014 and September 2017 and there was no evidence that any of them had been reviewed • although 13 documents had an assigned owner, for 10 of these it was a named individual rather than a job title • nine of the documents had no version number so it was not clear whether this was the most up to date version • there was no change history on any of the 18 documents reviewed, although nine of the documents were version 1.0 so no changes had yet been made. This is something that the ICO look for when they carry out reviews of Data Protection within organisations. Although we were made aware that HFRS are planning to review IT policies and procedures in preparation for GDPR implementation and as part of the transfer of documents to SharePoint, it is clear that several of the documents have not been reviewed for some time and therefore may be out of date and of limited value.			
Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
3.1	New Information Governance Policy	H	Performance Review Manager	July 2018
3.2	Existing policies and procedures transferred to new templates	M	Performance Review Manager	September 2018
Auditor's assessment of management response:				

Action plan 4 - Data Protection training within systems training				
Objective	Training and awareness for information management is comprehensive and periodically conducted for all new and existing staff.			
Observation	There is currently no general Data Protection training in place for all staff at HFRS. We were informed that Data Protection training was delivered to all staff, both operational and support, three years ago, however there has been no follow up to this. Additionally, Data Protection is not included in the induction process for new staff. This could lead to the mishandling of data, with the potential for data breaches leading to a fine. A Data Protection training package has been purchased, but at the time of the audit there had been technical issues which meant it had not been released for completion by all staff. HFRS collects personal data via two main systems, CFRMIS and FireWatch. CFRMIS is used by staff involved with safeguarding activities, so it contains sensitive personal data, and the safeguarding training received by them includes Data Protection and information sharing. However, we were informed by the FireWatch system owner that any training on FireWatch focuses on the functionality of the system, and Data Protection is not included. This increases the risk that lack of Data Protection awareness could lead to data breaches or data being incorrectly maintained.			
Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
4.1	Electronic Training for all staff to be delivered	H	Data Protection Officer	July 2018
Auditor's assessment of management response:				

Action plan 5 - Publication of FOI responses.	
Objective	Freedom of Information and Subject Access Requests (SAR) are dealt with in line with legislative requirements.
Observation	The HFRS procedure for processing Freedom of Information (FOI) requests requires a redacted copy of the response letter and the information sent to be uploaded to the FOI log on the HFRS internet pages. However, testing of a sample of 15 FOI requests completed between December 2016 and November 2017 highlighted that only the five completed requests from December 2016 to March 2017 had been uploaded. Further examination of the FOI log spreadsheet, and the published FOI responses, highlighted that only two responses out of 88 completed requests between April and November 2017 had been uploaded to the internet. Therefore HFRS are not complying with their processes.

	This could result in multiple requests for the same information which creates more work for the Knowledge Management Team.			
Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
5.1	These are now published on the website and procedure re-enforced accordingly	L	Information Compliance Officer	July 2018
Auditor's assessment of management response:				

Action plan 6 - Freedom of Information training for HFRS staff	
Objective	Freedom of Information and Subject Access Requests (SAR) are dealt with in line with legislative requirements.
Observation	There is no Freedom of Information (FOI) training currently in place for staff. HFRS is considering purchasing an FOI e-learning package but this will not be completed until the Data Protection e-learning is implemented. There is a risk that FOI requests may not be handled correctly if staff are not aware of how to recognise an FOI request, or what to do if one is received.

Management action				
What		**Priority (H/M/L)**	**Responsible officer**	**Target date**
6.1	Training package to be created and delivered	L	Information Compliance Officer	December 2018
Auditor's assessment of management response:				

Action plan 7 - Overdue FOI responses	
Objective	Freedom of Information and Subject Access Requests (SAR) are dealt with in line with legislative requirements.
Observation	We tested the four responses between April and November 2017 that had been issued late to determine the reasons. We found that for one of the requests, the information had been sent back to the Assurance and Compliance Officer's inbox, and she had been on leave at this time. Although it was dealt with on her return, this made the response one day late. For the remaining three requests, the delays were all due to the information being received late from the relevant departments. Although the departments were given a deadline to return the information to the FOI Team, for two of the requests there were no reminders issued by FOI

	when this deadline had been reached. Instead, reminders were emailed once the 20 day deadline for issuing the response to the requester had been reached. If reminders are not issued to departments once the internal deadline for the receipt of the information by FOI is reached it is more likely that the 20 day response time for FOIs will be exceeded.

Management action

What		Priority (H/M/L)	Responsible officer	Target date
7.1	Appropriate escalation to be included in the FOI procedure	M	Information Compliance Officer	September 2018

Auditor's assessment of management response:

Action plan 8 - Complaints procedures.	
Objective	Freedom of Information and Subject Access Requests (SAR) are dealt with in line with legislative requirements.
Observation	Section 45 of the Freedom of Information Act deals with the handling of requests, and this includes the need for a complaints procedures to be established. The ICO Section 45 Code of Practice requires the complaints procedure to include certain criteria. Although HFRS has a complaints procedure publicised online that broadly meets these requirements, there are two exceptions: • the details on the web page do not include reference to the response to the complaint being required within 20 days • the web pages do not advise complainants that they have a right to contact the Information Commissioner's Office if still dissatisfied with the HFRS response. Failure to comply with the ICO requirements could lead to further complaints.

Management action

What		Priority (H/M/L)	Responsible officer	Target date
8.1	Website to be updated with more detail to reflect the policy and procedure	L	Information Compliance Officer	Complete (May 2018)

Auditor's assessment of management response:

Action plan 9 - Public awareness of HFRS complaints procedure	
Objective	Freedom of Information and Subject Access Requests (SAR) are dealt

	with in line with legislative requirements.
Observation	When an FOI request is submitted to HFRS there are three ways in which the requester can be made aware of the complaints procedure: • details are on the FOI web page under "Feedback" • the acknowledgement template letter to the requester includes details of where to send any further correspondence, the complaints process and the ICO address to raise issues if not satisfied • the response template letter also includes details of where to send any further correspondence, the complaints process and the ICO address to raise issues if not satisfied. However, our testing highlighted that an acknowledgement letter was not on file for one of the 15 requests tested, and no response letter was on file for three of the requests. Additionally, one of the requests had been dealt with by Media and Comms, who do not have access to the template letters used by the FOI team. Therefore there is a risk that people submitting requests may not be informed of the complaints procedure.

Management action

	What	**Priority (H/M/L)**	**Responsible officer**	**Target date**
9.1	All FOIs are to be managed through the correct procedure and all relevant stakeholders to be notified.	M	Information Compliance Officer	Complete (May 2018)

Auditor's assessment of management response:

Action plan 10 - Disposal of IT equipment	
Objective	Data handling, storage, processing and destruction is in line with the 8 Data Protection principles.
Observation	We selected a sample of 11 items from the lists supplied by Jamie's Computers (the authorised disposal company) to the asset register on Hornbill. We were unable to find the record on Hornbill for one of the items selected - HFRS 0684 Compaq base unit. We also found that one Dell base unit (HFRSPC72) was still on Hornbill as being allocated to Fordingbridge Fire Station. We then selected ten items recorded in Hornbill as disposed of, and checked them to the Jamie's Computers lists, and could not find two items (Dell Laptop HFRSL303 and HP PRobook laptop HFRSL229). A failure to keep accurate records of IT hardware could result in losses being unidentified and a financial loss to the service. This could also result in a potential data breach.

Management action

What		Priority (H/M/L)	Responsible officer	Target date
10.1	Monthly audits of scrap equipment to be introduced	M	IT Security Officer	September 2018
Auditor's assessment of management response:				

Action plan 11 - Recording of data breaches	
Objective	Data handling, storage, processing and destruction is in line with the 8 Data Protection principles.
Observation	There is a Data Breach Log in place that is used to record any data breaches/incidents reported to the Knowledge Management Team. If a breach or incident is reported to IT this is recorded on Hornbill, and the Data Incident and Data Protection Breach procedures require an annual reconciliation between the Knowledge Management Team's records and Hornbill to ensure all data breaches are recorded on the log. The Data Breach Log requires the following details to be recorded to demonstrate compliance with the procedures: • breach reference (assigned by HFRS) • date received • topic • number of people (not completed for all three of the sample tested) • raised with • additional comments • conclusion • action taken • lessons learnt • breach/data incident • type of breach • disciplinary action taken (yes or no) • reported to the ICO. Testing of three data breaches recorded on the log identified the only details recorded were the reference, topic and person raised with - no further details were recorded. Additionally, all documentation associated with the breach, including the initial reporting of it and any evidence of investigation, should be held in a folder in SharePoint. Although there were ten breaches/incidents recorded in the log, there were only folders for incidents one to four in SharePoint. Therefore there was no evidence that a proper process had been followed for six of the data incidents/breaches recorded. This could leave HFRS exposed should the ICO become involved in investigating a breach.
Management action	

What		Priority (H/M/L)	Responsible officer	Target date
11.1	New procedure to be created and implemented	H	Data Protection Officer	September 2018
Auditor's assessment of management response:				

Action plan 12 – Data privacy impact assessments	
Objective	Privacy impact assessments are undertaken when changes are made to systems, policies and procedures.
Observation	The Project Lifecycle process requires all projects to have a Privacy Impact Assessment (PIA) completed for the project as part of the business case prior to this being submitted to the HFRS Senior Management Team (if under £100k) or HFRA (if over £100k) for approval at gate 2. The Programme and Project Management 'How to....Guide' also details the activities for which a PIA is required. A template is available to staff to assist them in this. We reviewed the documentation in place to support the drone project, and were unable to find any evidence that a PIA had been completed for this project. An on-line impact assessment had been completed, but this only includes the impact on people (equalities), health and safety, resources and environment. As part of the General Data Protection Regulation, Data Privacy Impact Assessments will become mandatory where the use of personal data is likely to result in high risk to the rights of the data subjects. Data Privacy Impact Assessments form part of the privacy by design aspect of the new legislation, therefore it is crucial to complete these for each new or revised data processing function.

Management action

What		Priority (H/M/L)	Responsible officer	Target date
12.1	Review of impact assessments to be completed and embedded within daily working practices	M	Performance Review Manager	April 2019
Auditor's assessment of management response:				

RECOMMENDATION

1. That the Standards and Governance Committee note our performance in respect of Information Governance.

BACKGROUND PAPERS

Guide to the General Data Protection Regulation (GDPR) – Information Commissioners Office
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

Contact:

Samuel Fairman, Performance Review Manager, Samuel.fairman@hantsfire.gov.uk, 07918 887502

Annex A

Key

The following is the key to quantify observations identified in the audit:

Assurance levels

Opinion	Framework of governance, risk management and management control
Substantial assurance	A sound framework of internal control is in place and is operating effectively. No risks to the achievement of system objectives have been identified.
Adequate assurance	Basically a sound framework of internal control with opportunities to improve controls and / or compliance with the control framework. No significant risks to the achievement of system objectives have been identified.
Limited assurance	Significant weakness identified in the framework of internal control and / or compliance with the control framework which could place the achievement of system objectives at risk.
No assurance	Fundamental weakness identified in the framework of internal control or the framework is ineffective or absent with significant risks to the achievement of system objectives.

Priority

Priority rating	Current risk
High	A significant risk of; failure to achieve objectives; fraud or impropriety; system breakdown; loss; or qualification of the accounts by the organisation's external auditors. Such risk could lead to adverse impact on the organisation or expose the organisation to criticism.
Medium	A serious, but not immediate risk of: failure to achieve objectives; system breakdown; or loss.
Low	Areas that individually have no major impact, but where management would benefit from improved risk management and / or have the opportunity to achieve greater efficiency and / or effectiveness.

Annex B

Assignment – Progress Control Sheet

Assignment stage	Assignment Progress				Comments
Audit Outline	Issued	10/10/2017	Agreed	10/10/2017	
Fieldwork commenced	Target	16/10/2017	Actual	20/10/2017	
Fieldwork completed	Target	19/01/2018	Actual	22/03/2018	Delays with obtaining information requested, also workloads of key HFRS staff made it difficult to schedule meetings for testing purposes.
Close of audit meeting	Target	26/01/2018	Actual	11/04/2018	
Draft Report Issued	Target[1]	25/04/2018	Actual	21/05/2018	
Factual accuracy agreed and management response provided	Requested[2]	04/06/2018	Provided		
Draft final report issued	Target[3]	11/06/2018	Actual		
Senior management sign-off	Requested[4]	18/06/2018	Provided		
Final report issued	Target[5]	20/06/2018	Actual		

[1] Within 10 working days of close of audit meeting

[2] Within 10 working days of draft report issued

[3] Within 5 working days of receipt of management response

[4] Within 5 working days of draft final report issued

[5] Within 2 working days of senior management sign-off