NORTH YORKSHIRE
FIRE & RESCUE SERVICE

Policies and Procedures

North Yorkshire Fire and Rescue Service

Internal Audit Report 2021/22

Business Unit: Enable North Yorkshire
Responsible Officer: MD Enable North Yorkshire
Service Manager: Business Design and Assurance
Date Issued: 10 February 2022
Status: Final
Reference: 45576/001

	P1	P2	P3
Actions	**0**	**3**	**2**
Overall Audit Opinion	Limited Assurance		

Veritau

Summary and Overall Conclusions

Introduction

In November 2018 the governance of the North Yorkshire Fire and Rescue Service (NYFRS) passed to the North Yorkshire Police, Fire and Crime Commissioner. In February 2020 the Commissioner approved a formal collaboration to bring together the business support functions for North Yorkshire Police and NYFRS, to be called 'Enable North Yorkshire'.

The formation of 'Enable North Yorkshire' led to a restructure of the administration functions of NYFRS, which was previously headed by the Central Administration Office (CAO). Until June 2021 the CAO were responsible for all NYFRS Policies and Procedures, ensuring they were being reviewed and updated within appropriate timescales. Each document were allocated to either a function or section area, with the appropriate Function Head allocated as responsible officer. Until April 2020 the Information Governance Group had an oversight of the whole process. This oversight transferred to the Tactical Leadership Team (TLT) under the new governance arrangements.

The service has a Records Management Policy and a Retention Schedule which sets out the timescales for policy review that needed to be followed. The management of records is governed by Section 46 of the Lord Chancellor's Code of Practice. Section 37 of the code sets out that the service should know what records it holds and where they are. It should ensure records remain usable for as long as they are required. Procedures within NYFRS are identified as SOP (Standard Operating Procedures). Policies and SOP's are stored in the Service Document area on the Sharepoint system. The Government requires Fire and Rescue services to adopt national operational guidance, and this will mean operational policies and procedures already in place will reflect or align to national operational guidance. Where there are local arrangements that supplement National Operational Guidance then an Operational Information Note should be written

It has been recognised by NYFRS and Enable management that policies and procedures and other service documents at NYFRS have not fully kept pace with the recent governance changes that have taken place. Some policies and procedures will relate to the governance and administrative functions but there is also concern some operational policies and procedures will not have been updated. By not updating the policies and procedures to reflect current legislation and practice, it is felt the present organisation is being put at risk.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system would ensure that:

- the management process for publishing, reviewing and monitoring documents was effective. This included the opportunity to Standardise, Simplify and Share existing arrangements within North Yorkshire Police
- the Records Management policy and Retention schedule were fit for purpose, up to date, and were being followed
- the Service had identified all the policies and procedures that were out of date
- those out of date policies that are putting the organisation at risk had been identified and the updating was being prioritised

The operational documents that were being reviewed by the Head of Response and Resilience were out of the scope of this work. Fieldwork was completed in the final quarter of 2021, and a draft report issued to management in December 2021.

Key Findings

We found a number of weaknesses around the effectiveness of the processes applied in the service, all of which show there is a need for a more rigorous control structure to be put into place. When discussing these matters during the work with the Head of Business Design and Assurance (EnableNY) there was awareness these areas needed to be addressed and the findings from the audit will help the service to focus/direct actions to progress these in 2022. There is a need to update all of the documents within the service document area on Sharepoint to reflect the new structure, including those documents that are not yet due for review.

The Records Management Policy and Retention Schedule are both overdue review and do not reflect the governance, system and procedural changes that have taken place to the service since 2018. The Records Management Policy has not been changed since 2016; It was last due a review on the 21 September 2021. Retention Schedule was due a review on the 15 January 2021, having been last reviewed on 15 January 2019. The basis of the documents are compliant with legislation, however, the Policy and Schedule are no longer fit for purpose and are in need of amendment to reflect the governance, system and procedural changes.

Within the service documents there is a SOPS Production and Issue Policy (review due 16 January 2021), which sets out guidance that any review period should be between 6 months and 5 years. Certain review periods can be governed by the Retention Schedule which sets out the legal expectations relating to certain documents and these are the maximum period between reviews. However there is no guidance in respect of the setting of the frequency of the review period. There is also no guidance to the operational production, issuing and reviewing of policies. Five years is a long period to set for a review for any type of service document and this would likely benefit from being reduced. An updated Records Management Policy is required that incorporates the production, issuing, review, retention and disposal of policies and procedures, which also could be standardised across both the Police and Fire services so that Enable Business Insight are working to common standards. There is also opportunity for some of the more generic service documents to be made applicable and accessible to both the Police and Fire. This is presently work in progress but is subject to the permission of the Home Office. ICT are presently trialling a shared drive on Sharepoint.

There were a large number of service documents that were out of date, one document that was duplicated under two headings (Safeguarding Referral procedure and Safeguarding Adults Procedure) and one document that was misfiled (Gender Pay Report 2019). All these documents had been identified in the NYFRS out of date service documents report dated 1 November 2021.

We reviewed the out of date policies and procedures and classified them as to the urgency of any review based on the risk to the organisation. Details of these documents have been provided to the Head of Business Design and Assurance. The RIPA Policy which was due for review on 11 May 2017, was the oldest document, with 7 other security documents such as the Whistleblowing Policy (28 March 2019), Anti-Fraud and Corruption (1 February 2020) and Information Security and Handling (15 January 2021) being in need of urgent review.

There are controls within Sharepoint round the 'checking out' and 'checking in' of service documents. During a review a document should be 'checked out', meaning that document can be worked upon with only the original version still being live to staff members to view.

Any document cannot be 'checked in' to the system until authorised by a Section Head, Function Head or designated administration staff. However, we found that where a document has been checked in by a designated administration staff there is no audit trail of who has done the review just the name of the designated administration staff member. Except for a minority of documents such as the Record Management Policy, there is also no trail as to any changes made to the service document either during a review, or for any other reason on the document itself.

Overall Conclusions

Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Limited Assurance.

1. Policies and Standard Operating Procedures (SOPs) do not reflect the new organisational structure

Issue/Control Weakness	Risk
Documents within the service document area do not reflect the new structure.	Users will be misdirected leading to inefficiency.

Findings

It has been recognised at senior management level within EnableNY that the policies, procedures and other service documents in place at NYFRS have not fully kept pace with the recent governance changes that have taken place within the organisation.

One of the Group Managers is carrying out a review of all service documents that need to be integrated into the National Operational Guidance. This work must be completed by January 2022. Our work did not review those Response and Resilience operational documents, of which 85 were shown as out of date in the service documents report circulated on the 1 November 2021

We reviewed the 96 documents due for review with dates ranging from 2017 to 31 July 2021. Looking at the sections of Policies, SOP, or Risk Assessment there were a total of 518 documents on the system. This figure includes 31 People Services documents that are out of date but are presently being reviewed as part of the project to find those policy and procedures that have some commonality across both services. A number of these documents, whether or not needed to be reviewed purely on the grounds that the governance information within the document was no longer relevant. However, these changes in the governance of the organisation will also effect all service documents whether due for review or not.

Agreed Action 1.1

All policies and standard operating procedures (SOPs) will be aligned to the revised service structures and amended to reflect the correct governance and responsible roles. Those responsible for policies and SOPs will be required to update them where required.	**Priority** 2 **Responsible Officer** Head of Business Design & Assurance **Timescale** 31 August 2022

2. Records Management policy and Retention schedule

Issue/Control Weakness	Risk
The Records Management Policy and Retention Schedule are both overdue review and do not reflect the governance, system and procedural changes that have taken place to the service since 2018.	Records Management Policy and Retention Schedule are not fit for the new organisation and are not compliant with the code of practice. The service could be at risk of sanctions from the Information Commissioners.

Findings

The management of records is governed by Section 46 of the Lord Chancellor's Code of Practice. Section 37 of the code sets out that the organisation should know what records it holds and where they are. It should ensure records remain usable for as long as they are required.

To ensure compliance with this code of practice the Service have a Records Management Policy and a Retention Schedule. The Records Management Policy sets out the aims of the Records Management System, the system and responsibilities. The Policy also outlines those systems used within the service, identifying Sharepoint on the intranet as forming the Electronic Documents and Records Management System. A further section identifies those other systems that are used to keep records, such as the Fire Watch. The Retention Schedule is an excel document and covers all types of records likely to be used by the service. On the CAO tab, all policies and procedures once superseded will be archived permanently electronically and all other copies destroyed by the CAO SI.

The Records Management Policy has not been changed since 2016. It was last due a review on the 21 September 2021, having been last reviewed on 13 September 2019. The documents version control shows the last amendment to the Policy, other than reviews, was made on 15 February 2016. The Retention Schedule was due a review on the 15 January 2021, having been last reviewed on 15 January 2019. The basis of the documents are compliant with legislation, however, the Policy and Schedule are no longer fit for purpose and are in need of amendment to reflect the governance, system and procedural changes. With the large number of out of date service documents we cannot give assurance that the policy and schedule have been followed.

Agreed Action 2.1

The Records Management Policy and Retention Schedule will be reviewed and revised to include current governance arrangements to ensure it complies with the Code of Practice and to provide meaningful support and advice to those responsible for records management.	**Priority** 2 **Responsible Officer** Head of Business Design & Assurance **Timescale** 31 August 2022

3. Policies relating to Policies, SOPs and Service Documents

Issue/Control Weakness	Risk
There is no operational guidance in place to cover the production, issuing and reviewing of policies, however there is one for SOPS. One set policy covering both services would improve efficiency and effectiveness of Business Insight in administrating the process.	Those creating Policies may not follow recognised procedures and a Policy may be published containing incorrect information.

Findings

Within the service documents there is a SOPS Production and Issue Policy (review due 16 January 2021). The Records Management Policy gives high level guidance to the production, issuing and retention of documents. The Records Management Policy is relied upon to give guidance towards the production, issuing and retention of documents including Policies. However, it does not go into the operational detail about the production, issuing and review of Policies to the extent that the SOPS Production and Issue Policy does.

A link within the SOPS Production and Issue Policy takes you to some guidance from the IT department entitled 'Creating, Approving, Publishing and Amending Service Documents'. This document is also available in service documents on the sharepoint system

The SOPS Production and Issue Policy has a 'Production of a SOP' section which covers liaison with all linked departments to ensure the SOP meets all relevant information to meet legislative and health and safety requirements, requires checks with the Section Head to see if compliant with current policy and legislation, and consultation with other departments for further comments and views.

An updated Records Management Policy is required that also incorporates the production, issuing, review, retention and disposal of policies and procedures, this could be standardised across both the Police and Fire services so that Enable Business Insight are working to common standards. There is also an opportunity for some of the more generic service documents to be made applicable to both the Police and Fire. Accessing documents that can be shared is presently work in progress and is subject to the permission of the Home Office. ICT have been trialling a shared drive on Sharepoint.

Agreed Action 3.1

Operational guidance will be reviewed in conjunction with the Records Management Policy. Appropriate template documentation will also be created to ensure a consistent approach is used in the creation, approval and publication of Policies, SOPs and Service Documents. It must be noted that National Operational Guidance will be the default source of information for any guidance documentation.	**Priority**	3
	Responsible Officer	Head of Business Design & Assurance
	Timescale	31 August 2022

4. Process for dealing with out of date documents

Issue/Control Weakness	Risk
A number of service documents are in need of urgent review. Any processes or controls to ensure service documents are updated in a timely manner have been ineffective. No trail is in place to track any agreed delays.	The service may face action in court or an industrial tribunal because officers followed out of date procedures. The reputation of the service with the staff and the public may be tarnished.

Findings

Section 8 of the SOPS Production and Issue Policy clearly states that CAO circulate on a monthly basis a list of those service documents that require a review or are awaiting approval by the Heads of Service. It is their responsibility to take any required action. Presently this function is carried out by the Inspection Support Officer in Business Insight. Using the out of date service documents report circulated on the 1 November 2021 we reviewed each of the documents and RAG rated them according to risk. The risks factors we considered included:

- potential legislative changes
- the potential impact on the organisation through following incorrect procedures
- the potential risk to the reputation of the service
- how far out of date a document was, alongside the set period a policy should be reviewed.
- the number of views that the document has had as recorded on Sharepoint. This gave us the number of views since Sharepoint online went live on 1 January 2020 or from the first date of publishing a new document.

From the report listing the out of date service documents we have identified that the RIPA Policy which was due for review on 11 May 2017, along with 7 other security documents such as the Whistleblowing Policy (28 March 2019), Anti-Fraud and Corruption (1 February 2020) and Information Security and Handling (15 January 2021) as being in need of urgent review. We have not been able to establish from the documentation that we have access to as to whether or not there are any reasons for the delays in updating these documents although we do understand that the fact as to whether the Fire service will continue to be subject to RIPA is awaiting a government decision. A number of People Services documents were also out of date however these are presently being reviewed to identifying those policies and procedures that have commonality between Police and Fire Services which can be stored in a shared area. Previously, this process was overseen by the Information Governance Group. Under the new structure this has been moved to the TLT. The previous system of reviewing policies and procedures relied heavily on the staff within the former CAO and this has led to weakness in controls around the reviewing and updating of documents.

Agreed Action 4.1		
i. All Policies, SOPs and Service documents will be reviewed by Group Managers and Heads of Function in consideration of the business areas they are responsible for. ii. Clear templates will be created to ensure a consistent approach and format including clear dates for document review and retention. A dashboard will be developed to provide visibility and performance reporting to feed into the governance arrangements.	**Priority**	2
	Responsible Officer	i. Head of Assurance ii. Head of Business Design & Assurance
	Timescale	31 August 2022

5. Reviewing of Service Documents

Issue/Control Weakness	Risk
There is no guidance on how to review a policy or the setting of frequency of review period. The current maximum of 5 years review period is considered too long. There is no trail back to who has actually reviewed the document, the decisions taken for review period or what was changed, if anything, during the review. No version control on service documents.	Documents may fail to comply with new laws and regulations. Documents may not address new systems or technologies which can result in inconsistent practice.

Findings

The 'SOPS Production and Issue Policy' states that a review period should be set between 6 months to 5 years, or when information is received that necessitates a review of the procedure. Section 3 sets out how a SOP should be reviewed, including the review be done by a suitably qualified person and include all relevant departments in the process to obtain their comments, views, and legislative changes. When completed the Section Head needs to review and agree the new SOP. Although not recorded in any policy document it was explained to us that a similar process would be followed when reviewing a policy. When starting a review a document is 'checked out' of Sharepoint; the original version remains available to all staff but any 'work in progress' version will not be live on Sharepoint.

The work in progress document is called a minor version. The control within Sharepoint in that any document cannot be 'checked in' to the system as a major document until authorised by a Head of Service or designated administration staff. Only major documents are able to be viewed by all staff. However we found that where a document has been checked in by a designated administration staff there is no audit trail of who has done the review, just the name of the designated administration staff member.

We saw the review periods being set depended on who reviewed the policy. Some documents had different periods set over the years depending on the committee or person reviewing. There are no guidelines as to what criteria should be taken into account when setting a review period, which should be linked to the risks to the organisation. It is felt a 5 year review period is too long and should be reduced. There was no accessible trail so we could consider the reasons behind the setting of a review period. Except for a minority of documents such as the Records Management Policy, there is no audit trail to identify any changes made to the service document either during the review or for any other reason. Those minority of documents contained a full version control table within the document itself.

Agreed Action 5.1		
A review of the Records Management Policy and Retention Schedule will include clear instructions about how often a document should be reviewed. These instructions will take into consideration whether there is a continuing purpose to maintain the record, that the record is up to date and not excessive, that the record complies with any data protections requirements and data quality principles.	**Priority**	3
	Responsible Officer	Head of Business Design & Assurance
	Timescale	31 August 2022

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.