



THE POLICE, FIRE AND CRIME COMMISSIONER FOR NORTH
YORKSHIRE AND THE CHIEF CONSTABLE OF NORTH YORKSHIRE

Subject Access Requests

FINAL Internal audit report: 12.18/19

22 January 2019

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept
no responsibility or liability in respect of this report to any other party.



CONTENTS

1 Executive summary	2
2 Detailed findings	4
Appendix A: Scope	10
Appendix B: Further information.....	12
For further information contact	13

Debrief held 7 December 2018
Draft report issued 3 January 2019
Responses received 22 January 2019

Final report issued 22 January 2019

Internal audit team Daniel Harris, Head of Internal Audit
Angela Ward, Senior Manager
Philip Church, Client Manager
Dominic Davis, Senior Auditor

Client sponsor Interim Chief Executive Officer
Chief Constable
Force Solicitor and Head of Legal Services
Police Lawyer (Civil Disclosure)

Distribution Interim Chief Executive Officer
Chief Constable
Force Solicitor and Head of Legal Services
Police Lawyer (Civil Disclosure)

1 EXECUTIVE SUMMARY

1.1 Background

A review of the subject access request process was undertaken at the Police, Fire and Crime Commissioner for North Yorkshire and the Chief Constable of North Yorkshire as part of the approved 2018 / 2019 internal audit plan.

Individuals have a right of access to their personal information held by organisations relating to them to help them understand how and why organisations are using their data and that they are doing so lawfully. This can be done by submitting a subject access request to the organisation in question, following receipt of a subject access request an organisation has one calendar month to respond. Failure to comply with these statutory deadlines can lead to fines and sanctions from the Information Commissioners Officer (ICO).

Subject access requests for both the Force and the Police, Fire and Crime Commissioner are received and responded to by the Civil Disclosure Unit, which sits within the Legal Services team. Since the introduction of GDPR in May 2018, the Civil Disclosure Unit has seen the number of subject access requests increase from 89 in the first two quarters of 2017/18 to 121 in the same period of 2018/19. Current compliance with the statutory deadline of responding to requests within one calendar month is 73% based on figures prepared for the period July 2018 - September 2018. Internal Audit have previously undertaken a review of the Freedom of Information process which is also carried out by the Civil Disclosure Unit which highlighted compliance in 2018/19 with the statutory deadline to be 59%. Consistent non-compliance with the deadlines could result in fines and intervention by the ICO.

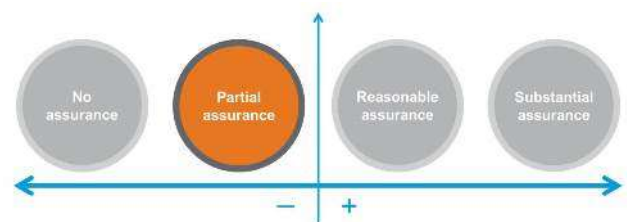
1.2 Conclusion

Through our review of the subject access request process, we found that in general, controls around the logging, processing and responding to requests to be working effectively, however we have raised concerns regarding the level of compliance with the statutory one-month deadline. The root cause of this appears to be the high level of requests being received by the team, coupled with a number of competing priorities within the Civil Disclosure Unit.

We have agreed **one high, two medium and three low** priority management actions as a result of our findings.

Internal audit opinion:

Taking account of the issues identified, the Police, Fire and Crime Commissioner for North Yorkshire and the Chief Constable of North Yorkshire can take **partial assurance** that the controls to manage this risk are suitably designed and consistently applied. Action is needed to strengthen the control framework to manage the identified risk.



1.3 Key findings

We have highlighted the following areas where controls are operating effectively:

- For our sample of 15 subject access requests we found that all were accompanied by two forms of ID, which adequately confirmed the ID of the data subject.
- All requests within our sample of 15 were logged on the system within two days of the request being made.

- We reviewed three subject access requests which were rejected. In all three instances we found the reasons for rejection to be reasonable, as per ICO guidance. Furthermore, the individual making the requesting had been informed in timely basis of the reason the request was being rejected.
- We reviewed the one instance since May 2018 of a third party request being made. In this instance we were satisfied that checks had been carried out in relation to the consent of the data subject and also that checks had been carried out to confirm the relationship between the third party and the data subject.
- We reviewed the three internal reviews of the subject access request process carried out independently by the DPO. In all three cases we confirmed that redactions had been reviewed and where appropriate removed. In instances where a redaction had been removed this was highlighted to the data subject. Following the internal review, the data subject was informed of the outcome and a revised set of documents sent out.

We have however agreed **one high and two medium** priority actions detailed below. A further three low priority actions are discussed in more detail in section two within the main body of this report. In summary:

- From our sample of 15 subject access requests, three (20%) were completed after the statutory one-month deadline. Furthermore, upon reviewing the reported compliance statistics it was noted that compliance with the deadline is overall around 70-80%. The underlying cause of this would appear to be a number of competing priorities within the Civil Disclosure Unit, with the team responsible for processing court orders and freedom of information requests, alongside subject access requests. We selected a sample of ten requests which were closed more than one calendar month after being received. In five of these instances we were satisfied that there was an appropriate reason for the delay and that the applicant had been informed of the delay. However, in the remaining five instances, two were overdue by more than the extended deadline (additional two months), two were overdue but the applicant had not been informed until after original deadline had passed, and in the remaining instance no reason had been provided for the request being closed after the deadline. **(High)**
- The procedure states the Data Protection Officers will undertake regular sample testing on subject access requests to determine the basis of any exemptions and redactions. Discussions were held with the Data Protection Officer for the Chief Constable and it was highlighted that due to resourcing issues it has not been possible to carry out any sample testing in this area. **(Medium)**
- Compliance statistics relating to subject access requests are reported to the Information Assurance Board on a quarterly basis however exceptions do not feature at the Executive Board, who therefore do not have oversight of the compliance on a frequent basis. **(Medium)**

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non compliance with controls*		Agreed actions		
					Low	Medium	High
Risk 6790 - New Data Protection Legislation	2	(13)	4	(13)	3	2	1
Total					3	2	1

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
1	A Data Protection – Subject Access Procedure is in place covering the subject access request process which is available on the staff intranet.	Yes	No	<p>A Data Protection - Subject Access Procedure is in place which was updated in June 2018 and owned by the Force Solicitor and Head of Legal Services. The procedure, outlines, the rights of the subject and the process. The process includes information regarding: proof of ID, verbal requests, response period, third parties, excessive requests appeals and complaints. We confirmed that the procedure is available to all staff on the staff intranet.</p> <p>We did however identify one area not covered by the procedure. Subject access requests can be escalated to the Data Protection Officer (DPO) for an independent internal review in the event that the data subject is not satisfied with the response. From our review of the procedure we were unable to identify the process to be followed in this instance including the desired timeframe for completion and what the outcomes of the review should look like.</p>	Low	<p>The Data Protection – Subject Access Procedure will be updated to include the internal review process and escalation process.</p> <p>Implementation Date</p> <p>30 April 2019</p> <p>Responsible Officer</p> <p>Police Lawyer (Civil Disclosure) and Data</p>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																								
				<table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Internal reviews of subject access requests are not investigated appropriately or within a suitable timescale.</td> <td colspan="3">The process for undertaking internal reviews has not been defined within the policy.</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Internal reviews of subject access requests are not investigated appropriately or within a suitable timescale.			The process for undertaking internal reviews has not been defined within the policy.			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8		Protection Officer for the Chief Constable
Risk exposure			Root cause																											
Internal reviews of subject access requests are not investigated appropriately or within a suitable timescale.			The process for undertaking internal reviews has not been defined within the policy.																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
2	Subject access request forms are available at all police stations, NYP and OPFCC websites.	Yes	No	<p>We confirmed, that subject access request forms were available at the reception of the North Yorkshire Police HQ. Furthermore, a review of the North Yorkshire Police website shows that a PDF form is available to print as well as an online form available for completion.</p> <p>However, when we reviewed the Police, Fire and Crime Commissioner for North Yorkshire's (PFCC) website we were unable to locate a subject access request form.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">There is a delay in subject access requests from the Police, Fire and Crime Commissioner reaching the Civil Disclosure Unit</td> <td colspan="3">The PFCC website does not contain a subject access request form or a link to the e-form</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			There is a delay in subject access requests from the Police, Fire and Crime Commissioner reaching the Civil Disclosure Unit			The PFCC website does not contain a subject access request form or a link to the e-form			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8	Low	<p>The PFCC website will be updated to include a link to the subject access request form and e-form.</p> <p>Implementation Date</p> <p>30 April 2019</p> <p>Responsible Officer</p> <p>Data Protection Officer for PFCC</p>
Risk exposure			Root cause																											
There is a delay in subject access requests from the Police, Fire and Crime Commissioner reaching the Civil Disclosure Unit			The PFCC website does not contain a subject access request form or a link to the e-form																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
3	As per ICO guidelines, subject access requests are acted on within	Yes	No	<p>We took a sample of 15 subject access requests received since May 2018. Of these, three (20%) were not acted upon and closed within the statutory period of one calendar month. Furthermore, examination of compliance statistics reported to the Information Assurance Board shows that compliance with the statutory timescales is between 75 - 80% since May 2018. Failure to</p>	High	Resource to undertake subject access requests needs to be reviewed in																								

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																								
	one calendar month.			<p>consistently meet the SAR deadline could result in sanctions and penalties from the ICO.</p> <p>Discussions with staff within the team, managers and the Data Protection Officers all highlighted that capacity is a concern with regards to subject access requests. Currently responsibility for these requests sits with the Civil Disclosure Unit which have a number of competing priorities such as court orders and FOI requests, all of which have statutory deadlines to meet.</p> <p>Following the introduction of GDPR, subject access requests have risen from 89 in the period April - June 2017 to 121 in the same period in 2018. With several competing priorities as well as an increased number of requests it will be difficult to increase compliance with the statutory deadline which sits at 73% for the latest period reported (July 2018 - September 2018). Resourcing and responsibilities in relation to subject access requests is currently being considered as part of the Transform 2020 project being undertaken at NYP with a number of options currently being considered.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Subject access requests will not be responded to within one calendar month leading to investigation and possible fines from the ICO.</td> <td colspan="3">Subject access requests are handled by a small team of legal officers who have a number of competing priorities including FOI requests and court orders, each of which have demanding deadlines for completion.</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Subject access requests will not be responded to within one calendar month leading to investigation and possible fines from the ICO.			Subject access requests are handled by a small team of legal officers who have a number of competing priorities including FOI requests and court orders, each of which have demanding deadlines for completion.			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8		<p>order to increase the compliance rate.</p> <p>An assessment of resources required as well as where responsibility for subject access requests sits will be undertaken and potential options will be fed into the Transform 2020 project.</p> <p>Implementation Date</p> <p>31 December 2019</p> <p>Responsible Officer</p> <p>Force Solicitor and Head of Legal Services & Police Lawyer (Civil Disclosure Unit)</p>
Risk exposure			Root cause																											
Subject access requests will not be responded to within one calendar month leading to investigation and possible fines from the ICO.			Subject access requests are handled by a small team of legal officers who have a number of competing priorities including FOI requests and court orders, each of which have demanding deadlines for completion.																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
4	Complex or numerous requests may be able to	Yes	No	We reviewed a sample of 10 subject access requests which were closed after the statutory one-month deadline. In five instances we were satisfied that there	-	See action three above.																								

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																								
	<p>extend the response period by an additional two months.</p> <p>Where the one month statutory period will not be met, the applicant will be informed to advise them of the delay.</p>			<p>was a suitable reason for the delay and obtained evidence that the applicant had been informed of this delay.</p> <p>We identified five instances where there was either not a suitable reason or the subject had not been contacted informing them of a delay. In two of these instances the applicant was informed of the delay, but only after the initial deadline had passed. In a further two instances the request was overdue by more than the extended deadline and in one of these the subject has made a complaint to the ICO. In the final instance the request had gone overdue with no reason or communication to the subject.</p> <p>Failure to inform data subjects of any potential delay could result in complaints being made to the ICO. Furthermore, where requests significantly breach the one-calendar month timescale, this further increases the risk of action being taken by the ICO. The root cause of this links back to the resource issue highlighted within control and findings reported at number 3 above.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Individuals are not informed of any delays resulting in complaints to the ICO and potential investigation and fines by the ICO.</td> <td colspan="3">Subject access requests are handled by a small team of legal officers who have a number of competing priorities including Freedom of Information Requests and court orders, each of which have demanding deadlines for completion.</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Individuals are not informed of any delays resulting in complaints to the ICO and potential investigation and fines by the ICO.			Subject access requests are handled by a small team of legal officers who have a number of competing priorities including Freedom of Information Requests and court orders, each of which have demanding deadlines for completion.			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8		
Risk exposure			Root cause																											
Individuals are not informed of any delays resulting in complaints to the ICO and potential investigation and fines by the ICO.			Subject access requests are handled by a small team of legal officers who have a number of competing priorities including Freedom of Information Requests and court orders, each of which have demanding deadlines for completion.																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
5	On a regular basis the DPOs undertakes a	Yes	No	The procedure states the Data Protection Officers will undertake regular sample testing on subject access requests to determine the basis of any exemptions and redactions. Discussions were held with the Data Protection Officer for the	Medium	In the absence of resource working with the DPO it is difficult to prioritise these																								

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																								
	sample test of subject access requests to make sure they have been processed appropriately, the redactions made are justified and the exemptions clearly stated.			<p>Chief Constable and it was highlighted that due to resourcing issues it has not been possible to carry out any sample testing in this area. Sample testing by a member of staff independent of the SAR process would add value and by not carrying these out, there is a risk that inconsistencies in the process are not detected which could lead to future complaints by those who have submitted a SAR and not received suitable response.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Inconsistencies within the subject access process are not identified and mistakes continue to be made resulting in an increased number of complaints.</td> <td colspan="3">Lack of resource within the DPO team to be able to prioritise periodic reviews</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Inconsistencies within the subject access process are not identified and mistakes continue to be made resulting in an increased number of complaints.			Lack of resource within the DPO team to be able to prioritise periodic reviews			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8		<p>reviews, therefore the issue of resourcing will be considered as per action three.</p> <p>Implementation Date</p> <p>31 December 2019</p> <p>Responsible Officer</p> <p>Force Solicitor and Head of Legal Services & Police Lawyer (Civil Disclosure Unit)</p>
Risk exposure			Root cause																											
Inconsistencies within the subject access process are not identified and mistakes continue to be made resulting in an increased number of complaints.			Lack of resource within the DPO team to be able to prioritise periodic reviews																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
6	Should a SAR not be satisfactory resolved, the subject can request an independent review by the DPO.	Yes	No	<p>We reviewed the website as well as the subject access request forms and identified that the subjects right to an internal review had not been communicated.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Individuals are not made aware of their rights to an internal review</td> <td colspan="3">Internal review process not detailed on public facing information</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Individuals are not made aware of their rights to an internal review			Internal review process not detailed on public facing information			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8	Low	<p>Both websites as well as the subject access request form will be updated to include reference to the internal review process.</p> <p>Implementation Date</p> <p>30 April 2019</p> <p>Responsible Officer</p> <p>Data Protection Officer for the OPFCC</p>
Risk exposure			Root cause																											
Individuals are not made aware of their rights to an internal review			Internal review process not detailed on public facing information																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									
7	Missing Control	No	-	<p>Compliance statistics relating to subject access requests are reported to the Information Assurance Board on a quarterly basis however exceptions do not</p>	Medium	<p>As per the FOI process, Subject Access Requests</p>																								

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																								
	Compliance statistics relating to subject access requests are reported to the Executive Board.			<p>feature at the Executive Board, who therefore do not have oversight of the compliance on a frequent basis.</p> <p>Without reporting the levels of compliance to the Executive Board there is a risk that senior management are not aware of any issues relating to compliance and the risks faced should the force not comply with legislation.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk exposure</th> <th colspan="3">Root cause</th> </tr> </thead> <tbody> <tr> <td colspan="3">Staff in senior position are unaware of issues with compliance resulting in lack of oversight of issues which could carry significant threats of ICO investigation</td> <td colspan="3">Compliance statistics are not reported to the executive board on a regular basis.</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Negligible</td> <td>Minor</td> <td>Negligible</td> <td>5:8</td> </tr> </tbody> </table>	Risk exposure			Root cause			Staff in senior position are unaware of issues with compliance resulting in lack of oversight of issues which could carry significant threats of ICO investigation			Compliance statistics are not reported to the executive board on a regular basis.			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Negligible	Minor	Negligible	5:8		<p>should be reported to the Executive Board on an exception basis to ensure that the Executive Board are fully aware of issues relating to compliance (or non-compliance) with legislation.</p> <p>Implementation Date</p> <p>30 April 2019</p> <p>Responsible Officer</p> <p>Force Solicitor and Head of Legal Services</p>
Risk exposure			Root cause																											
Staff in senior position are unaware of issues with compliance resulting in lack of oversight of issues which could carry significant threats of ICO investigation			Compliance statistics are not reported to the executive board on a regular basis.																											
Probability	Financial	Reputational	Operational	Legal	Rating																									
Probable	Negligible	Negligible	Minor	Negligible	5:8																									

APPENDIX A: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
To ensure subject access requests have been processed in a timely manner and in accordance with article 15 of GDPR and s45 of Data Protection Act.	Risk 6790 - New Data Protection Legislation	Strategic Risk Register

When planning the audit the following areas for consideration and limitations were agreed:

Under article 15 of GDPR an individual has the right to obtain from a data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. In the advent of GDPR the organisations have seen an increase in subject access requests, as such our review will consider the following areas:

- Policies and procedures are in place, reflecting current operating practices.
- Subject access requests have been acted upon within at least 30 days of receipt.
- Appropriate ID - and authority where making the making the request on behalf of another - has been provided by the individual making the request
- Refusal of requests are appropriate and clearly communicated to the individual.
- When requests are manifestly unfounded or excessive a reasonable charge for the administrative costs of complying with the request has been applied.
- Extension of time to respond to requests are justified due to the complexity or a number of requests have been received from the individual. We will confirm that the individual has been made are of the extension within one month of receiving the request.
- Applications on behalf of any other person (third party) are supported by authorisation letter and proof of identification documents.

Limitations to the scope of the audit assignment:

- This review will focus on subject access requests only.
- Testing will be undertaken on a sample basis, so we will not confirm all subject access requests have been processed appropriately.

- Our review will not guarantee the outcome of a review undertaken by the ICO.
- We will not review the actions put in place to improve performance but only confirm performance is reported through the organisations' governance structures.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Interim Chief Executive Officer
- Fore Solicitor and Head of Legal Services Police Lawyer (Civil Disclosure)
- Data Protection Officer, the Police, Fire and Crime Commissioner
- Data Protection Officer, the Force
- Administrative Assistant (Civil Disclosure)
- Legal Officer (Civil Disclosure)

Documentation reviewed during the audit:

- Subject Access Procedure
- Subject Access Request Form
- SAR Report
- Subject Access Request Documentation within IKEN
- Information Assurance Board Statistics

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **the Police, Fire and Crime Commissioner for North Yorkshire and the Chief Constable of North Yorkshire**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.