

Police and Crime
Commissioner
North Yorkshire



Mobile Phone Examination Final Report

Auditor	Faye Simmons
Contact Details	Faye.Simmons@westyorkshire.pcc.pnn.gov.uk
Date of Review	June – October 2015
Draft Report Issued	28 th October 2015
Final Report Issued	11 th November 2015

1 Executive Summary

Mobile phones are an important source of information in the detection and disruption of criminals. Mobile phone examinations are currently undertaken by examiners at District Investigation Hubs, previously Safer Neighbourhoods Crime, and by staff at the HQ Mobile Phone Unit (MPU).

The examination of mobile phones at District level was reviewed as a part of the audit, focussing on mapping the current processes in place for the submission and examination of mobile phones by those individuals who are qualified. A sample of 50 mobile phone examinations undertaken from April 2014 – April 2015 at York, Scarborough and Harrogate were reviewed. It is acknowledged that the period reviewed as a part of the audit was prior to the creation of the Investigation Hubs and was when staff and officers came under Safer Neighbourhoods Crime (SNC).

Whilst the main focus of the audit was the procedure for a mobile phone examination, the return to owner process was also considered and was found to be adequate. Sufficient notification is given to the owner that the item can be returned to them and whilst only a small number of the mobile phones within the sample were appropriate to be returned to their original owner, reasonable assurance can be given that this process is being handled appropriately.

A summary of each key audit finding is summarised below:

Training

Training of staff at a District level was considered as a part of the review and whilst training has provided staff with the capability to undertake mobile phone examinations, issues have been raised with the way in which this training has been delivered. IA have been advised that staff at Districts have received training in using XRY from staff within the MPU and not a qualified trainer. Whilst having this level of training allows the examiner to provide reliable evidence in court, concern is raised over the assurances it can provide particularly where District staff investigate a more serious level of crime. It is the opinion of IA that a thorough assessment of resourcing and training requirements at Districts would be necessary to address issues with the training process.

Review of Serious Crimes

Force policy states that District examiners should not undertake investigations of more serious crimes due to the level of interrogation they are able to provide. However examiners do investigate these crimes, which affects the level of scrutiny that can be provided as a full download cannot be performed by District examiners. Whether the Mobile Phone Unit are made aware of this is not evident and if any assessment is taken of whether the examination was appropriate for Districts to complete. It would be suggested that the MPU undertake more regular dip sampling of District examinations, assessing the appropriateness of these examinations as well as other areas where examination procedure may not be being adequately followed and where necessary raise issues or concerns with the relevant DI.

Data Security

Where a successful download occurred a disk was present in the physical file. However 6/50 of the physical files containing the disk, FSD9 submission form, and Digital Media Examination form could not be located at Harrogate, Scarborough or York. As a result there is a risk that possibly sensitive data may have been lost or misappropriated and this raises wider issues around the overall security of extracted data. This was raised with staff at the time of the field work being completed.

Additional data security issues are also highlighted around the encryption of the extracted data. Initially IA were advised that whilst Districts have the capacity to encrypt data they do not use it. Given that storage of the data at Districts is in cabinets that are not always locked and could be accessed by members of staff outside of the Investigation Hub, encryption must be used to adequately safeguard extracted data.

District Processes

Of the sample of mobile phones that were reviewed, a number of issues were found in relation to file documentation that was held at the Districts. It was highlighted that 25/50 of the files examined did not have an FSD9 submission form providing evidence of the objectives of the investigation and of the Detective Inspector (DI) authorisation. Internal Audit were advised that these forms may be returned to Officer in the Case (OIC) with the examination data, however this is not evidenced through the Niche record. As this information isn't adequately evidenced it is difficult to provide assurances that DI authorisation has actually been received.

In 2/50 cases it was identified that a submission form was evident but DI authorisation had not been received. In these instances, according to procedure, the investigation should not have been performed. Particular good practice in this area was highlighted at Scarborough District, whereby the submission form was received electronically an email was sent to the appropriate DI to receive authorisation. Both the form and the email were adequately evidenced through the physical file. It is recommended that evidence such as this from the mobile phone examination is added to the Niche occurrence, as this is the primary recording method for used by the Force.

MPU Processes

Processes in place within the Mobile Phone Unit, particularly around how they manage their workload was assessed by IA. Whilst it is good practice that examinations are categorised upon receipt in the MPU based on certain crime types and a key date in the case (e.g. bail date) further measures need to be put in place to improve the efficiency of the MPU. For example a scoring matrix which would determine the severity of the interrogation and the priority level for examination. A similar system is already in use within the Hi-Tech Crime Unit and has potential to be adapted for MPU purposes.

Data Quality

Usage for the period 2012-2015 from the SNC spreadsheet provided to IA, also highlighted that the number of examinations at a local District level is on the increase from approximately 154 examinations in 2012 to 1210 examinations in 2014. This is to be expected as mobile phones become commonplace. However IA would raise a minor issue with the quality of the data provided by the SNC spreadsheet. A number of blanks are present in terms of crime type, examiner, authorising officer and which district undertook the investigation. A reminder should be issued to DI's about the need to appropriately complete this spreadsheet, thus providing the MPU with more detail of the examinations that are taking place.

Data held through the SNC spreadsheet was also matched against the record of the examination held on Niche, however these sources do not always match. Of the sample in terms of crime type 6/50 did not match, for date of seizure 5/50 and the date the phone was examined 14/50 did not match against the Niche record. More regular review against the Niche record would be deemed necessary to ensure that it accurately reflects examination detail and ensuring continuity of evidence, especially where documentation held at Districts may be insufficient.

Summary Opinion

Overall whilst it is beneficial to have examiners at districts, only limited assurance can be provided that procedure is being followed appropriately at a District level, particularly in relation to evidencing key examination documents and authorisation. Concern has also been raised regarding the overall security of examination data especially where this data relates to a more serious crime. It is therefore considered that further review by the MPU may be necessary to remedy control issues and ensure best practice.

	Commentary
Effectiveness of Risk Management Approach	The current approach at present highlights a number of areas where Force policy and procedure are not being adequately followed at a District level. As a result it is difficult to provide assurance that examinations particularly of more serious crimes, are being undertaken appropriately. The review also highlighted a number of weaknesses in MPU processes, as such recommendations have been made to address this.
Efficiency of Risk Management Approach	Whilst the current approach allows for the expedient examination of mobile phones, it is considered that sufficient review of examinations across Districts is not occurring. As a result more serious crimes are being investigated contrary to Force policy and without thorough consideration of subsequent data security.
Assurance Level	3 Limited Assurance
Overall Risk	3:13

2 Scope and Approach of the Audit

The audit will include Internal Audit mapping the current processes in place for the submission and examination of mobile phones to those individuals who are qualified in the Safer Neighbourhood units and the specialist HQ Mobile Phone Unit. In doing so the activity of the examination and submission will be reviewed and the following risks will be considered:

- Criminals may not be brought to justice due to evidence not being expediently investigated;
- Evidence and high risk material gained through examination could be lost or misappropriated;
- Processes and training currently in place to deal with mobile phone examinations may not be credible or provide sufficient integrity/competence to successfully prosecute individual and be effective;
- Material gained through examination pertaining to a crime, but not related to the original request, may not be investigated;
- And mobile phones subject to examinations may not be returned to the owner (when appropriate).

Each recommendation is accompanied by an assessment of the likelihood and impact of the risk identified, to North Yorkshire Police (NYP) as a whole.

3 Report Distribution

Name/Role	Draft	Final	Final with Response
Richard Cockerill, Digital Forensics Manager	✓	✓	✓
Detective Inspector Adrian Gathercole	✓	✓	✓
Detective Inspector Jim Glass	✓	✓	✓
Superintendent Alistair Dey	x	✓	✓
Chief Superintendent Simon Mason	x	✓	✓
Risk and Assurance Unit	x	✓	✓
Michael Porter, Police & Crime Commissioner's Chief Finance Officer	x	✓	✓
Jane Palmer, Chief Constable's Chief Finance Officer	x	✓	✓

4 Observations

4.1 Training

Risk Exposure			Root causes		
Training may not provide sufficient value to successfully prosecute an individual and be effective.			Not all examiners have received training from a qualified XRY trainer. Training updates are not regularly received.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Minor	Minor	Significant	3:13

Current usage data highlights that from March 2012 – April 2015 that 10 examiners of the 46 known users logged on the SNC spreadsheet accounted for 65% of all examinations undertaken through the period. A gap is therefore highlighted between training provided and the degree to which training is used. It is the opinion IA that review of resourcing and training needs could be considered to address training issues around how training has been delivered to District examiners.

IA have also been advised by the Training School at NYP that it is acceptable to receive training by an individual who is unqualified (if the head of training school is present) and this is acceptable for use in court. However it is considered that if the practice of District examiners undertaking review of more serious crimes is to continue then full and appropriate XRY training should be provided. At present concerns are raised over the benefit of extracted data provided by Districts for more serious crime as a full download is not performed. There is a risk that an individual may not be successfully prosecuted as a result and this raises issues around the value that District examinations can provide.

Consideration should be given to a review of training practices with the possibility of providing full XRY training to 20 individuals who regularly undertake mobile phone examinations. The training needs of these individuals can be more proactively monitored and managed particularly for when a person moves to a role that doesn't require this training or leaves the organisation. Where this is the case training can be more readily provided new examiners as needed.

Recommendation 1

Assessment should be undertaken of the current resourcing requirements of the District Investigation Hubs, reviewing where training updates may be required and where the training of new examiners may be necessary.

4.2 Serious Crime

Risk Exposure			Root causes		
Criminals may not be brought to justice as evidence for more serious crimes is not obtained from a mobile phone examination			More serious crimes are being investigated without the MPU having an awareness of this occurring.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Significant	Minor	Significant	3:13

Review of the usage of District examinations showed that 26% of examinations undertaken from 2012-2015 were serious crime types for example sexual offences and murder cases. Examiners at Districts should only investigate lesser crimes such as burglary, whereas the MPU should examine mobile phones for those crimes which are more serious and where a more comprehensive interrogation of the phone is required. Where these crimes are being interrogated by District examiners there is a risk that these phones will not be subject to the same level of scrutiny as they would if they were investigated by the MPU, reducing the value that mobile phone investigations can provide.

At the time of the audit IA were advised that when MPU resources are not available (e.g. on a weekend) a District examiner may undertake the investigation. However the MPU do not undertake sufficient review of where these more serious crimes have been examined by Districts. Whilst it is not always practicable for the MPU to authorise these investigations, it is necessary that they have more of an awareness of what examinations are taking place. It would be recommended that procedure be updated so that in exceptional circumstances Districts can undertake interrogations of more serious crimes. A system of regular dip sampling by the MPU is also recommended to ensure that review of serious crimes is appropriate and that the overall examination process is being appropriately followed.

Further to this it has been highlighted that the FSD9 submission form is not always evidenced, this a particular issue for more serious crimes. The form should provide a rationale behind why the examination was considered necessary and also that DI authorisation was actually granted. It is the opinion of IA that where a more serious crime was examined that some justification of why this was deemed appropriate should be provided. This can then be subject to further dip sampling undertaken by the MPU.

Recommendation 2

The Mobile Phone Unit should undertake regular dip sampling of District level examinations, focussing on the types of crime reviewed and the appropriateness of the District undertaking them.

Recommendation 3

Policy should include exceptional circumstances whereby the Districts can review more serious crimes when the MPU is not available.

4.3 Data Security

Risk Exposure			Root causes		
Data from the mobile phone download may be lost or misappropriated			Data pertaining to more serious crimes is not encrypted. Data is not securely held within the District Investigation Hubs.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Significant	Minor	Significant	3:13

Concern is raised where data is not encrypted, given that more serious crimes are being investigated there is an increased risk that sensitive data may be lost or misappropriated. IA have been advised that District examiners have the capacity to encrypt data but do not utilise this. Given that the MPU and external firms used by NYP for mobile phone examinations encrypt data, it would be considered appropriate for District examiners to undertake this also in order to mitigate the risks associated with the security of extracted data.

Through the course of the review it was highlighted that a number of physical files containing the disk, FSD9 submission form and Digital Media Examination form could not be located and a number of these related to more serious crimes, raising wider issues around the security of extracted data. The data within the Investigation Hubs is held in cabinets that are not always locked and could be accessed by staff who aren't based within the Hubs. Encryption of the extracted data would therefore mitigate the risks associated with this.

Further to this the delivery of the extracted data is passed through internal mail, however notification of delivery does not occur therefore data security could be compromised. It was highlighted that Districts often prompt the OIC to attend the Investigation Hub and collect the data directly, which is better practice for ensuring appropriate data security.

Recommendation 4

District procedure should include the necessity to encrypt all extracted data.

Recommendation 5

Issue a reminder to District examiners of the need to ensure the security of extracted data. Including where extracted data has been sent via internal mail, receiving confirmation from the OIC that the data has been received.

4.4 Scoring Matrix

Risk Exposure			Root causes		
A mobile phone may not be investigated by the key date in the case.			The MPU does not have a formal scoring matrix in place.		
			The MPU works with a back log of examinations.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Minor	Minor	Minor	5:8

Through discussions within the MPU, it has been identified that a formal system of prioritising investigations is not being used. Whilst a system of categorising investigations by crime type upon their arrival to the unit is already in use, further action can be taken to prioritise mobile phone examinations and therefore reduce any back log that may be in place.

A scoring matrix can take into account key factors such as crime type, key date and material to be examined, to provide a score as a basis for prioritising a particular examination over another. It is considered that this is a more efficient method of handling the workload of the MPU. The MPU already utilises a system for high priority work and undertakes regular review of outstanding work, the scoring matrix would better embed this into MPU procedures.

Furthermore the benefit of scoring matrix is that a low scoring examination could be referred as appropriate for District examiners to undertake. This would reduce the risk of a back log occurring and that deadlines for a more serious examination may be missed. This would also be a more effective system as the MPU can place more focus on more serious examinations, increasing the value of the service they provide to officers.

A system similar to this is already in place within the Hi-Tech Crime Unit, therefore it may be the case to adapt the scoring matrix they have within the department for the purposes of the MPU.

Recommendation 6

For the initial scoring of MPU examinations to be undertaken, to ascertain their priority level and ensure the log of outstanding examinations is regularly monitored and reviewed as continued good practice.

4.5 FSD9 Submission Form

Risk Exposure			Root causes		
DI authorisation is not received for an investigation.			The FSD9 Submission Forms are not always evidenced by Districts.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Negligible	Minor	Negligible	5:8

In 25/50 examination files an FSD9 submission form was not evidenced, as a result limited assurance can be provided that the examination was undertaken in compliance with Force procedure. The form should evidence that DI authorisation has been received, that the phone has appropriate grounds to be examined and what the interrogation of the mobile phone is going to achieve.

IA were advised that it may be the case that the form is returned to the OIC to be evidenced as a part of the case file. However it is still important for the each District to have a copy for their own records, as the OIC does not always evidence this form through Niche.

Given that Niche is the primary method for recording criminal investigations, it would be beneficial to the quality of the case file to scan associated mobile phone information onto the Niche occurrence. It would be more efficient to record examination in this way, as the OIC, the examiner and the MPU can access the information if needed. This also reduces the need to maintain paper documentation at Districts, reducing the risk of data security issues.

Current procedure only specifies the requirement to evidence the disk of the extraction and the notes, consideration should be given to specific requirements for providing evidence of an examination performed at a District level.

Recommendation 7

Current procedure should be updated to include the requirement for the FSD9 submission form and Digital Media Examination to be scanned on to the Niche record of an occurrence.

4.6 Data Quality

Risk Exposure			Root causes		
Information pertaining to the investigation on the Niche record is not accurate.			The SNC spreadsheet is not always completed fully with examination information.		
Probability	Financial	Reputation	Operational	Legal	Rating
Probable	Negligible	Negligible	Minor	Minor	5:8

The review mapped data from the SNC spreadsheet of District investigations across to the Niche occurrence. It has been highlighted that in 28% of cases examined the date the mobile phone was examined did not match on the two records. IA also found discrepancies in crime type and the date the mobile phone was seized and whilst crime type discrepancies can be explained through changes through the course of the investigation, discrepancies in date seized or date examined raise issues around how continuity of evidence is maintained.

The Niche record should keep an accurate record of the mobile phone and discs location, ensuring that continuity of evidence is maintained. It is recommended that the OIC and the examiner must keep examination information such as the submission form and returns form on the Niche record, as at present this does not occur.

The SNC spreadsheet is also not always completed, with a number of gaps including the examiner who performed the examination, the authorising officer, and the date the phone examination took place.

If the SNC spreadsheet is to continue to be used to log District examinations then the MPU should review the SNC spreadsheet and map information towards Niche to review the accuracy of the information recorded. As a part of dip sampling that has been recommended the MPU should consider mapping information from the SNC spreadsheet across to Niche to ensure accuracy of records is maintained. It would also be necessary to remind DI's of the need to complete this spreadsheet appropriately, liaising with the examiner to ensure that the information submitted is correct.

Recommendation 8

Detective Inspectors should be appropriately reminded of the need to complete the SNC

NOT PROTECTIVELY MARKED

Final
spreadsheet for mobile phone examinations, liaising with OIC and District examiner where further detail may be needed.

#	Recommendation	Category of Rec.	Management Action	Action Manager & Completion Date	Satisfactory Response (IA View)
1	Assessment should be undertaken of the current resourcing requirements of the District Investigation Hubs, reviewing where training updates may be required and where the training of new examiners may be necessary.	Significant	The Forensic Science Regulator has recently announced the scope of the requirements for regulation of Digital Forensics. This will include area based mobile phone examinations. The requirements fall under the International Standards Organisations standard 17025. Introduction of 17025 is being managed by Richard Cockerill and Mark Bates. A paper is currently being prepared for the Command Team and will include the requirements to employ a Quality Manager who will ensure that policies are up to date and will audit adherence to them. Compliance will be reviewed by the UK Accreditation Service UKAS. Training will be included within the requirements. This is expected to be in place by July 2016 with mandatory formal accreditation by October 2017	Richard Cockerill Digital Forensics Manager July 2016	
2	The Mobile Phone Unit should undertake regular dip sampling of District level examinations, focussing on the types of crime reviewed and the appropriateness of the District undertaking them.	Significant	ISO17025 will require a review of procedures and formal internal auditing of compliance	Richard Cockerill Digital Forensics Manager July 2016	

NOT PROTECTIVELY MARKED

Final

3	Policy should include exceptional circumstances whereby the Districts can review more serious crimes when the MPU is not available.	Significant	Guidance has recently been issued extending the circumstances in which districts can review mobile phones. This will be published in the updated procedure referred to above.	Richard Cockerill Digital Forensics Manager July 2016	
4	District procedure should include the necessity to encrypt all extracted data.	Significant	Richard Cockerill will ensure that area kiosk equipment is configured in such a way that all output is encrypted. This will be included in the above procedures.	Richard Cockerill Digital Forensics Manager January 2016	
5	Issue a reminder to District examiners of the need to ensure the security of extracted data. Including where extracted data has been sent via internal mail, receiving confirmation from the OIC that the data has been received.	Significant	Richard Cockerill is to further remind staff of the need to ensure security of extracted data. The requirement is to be included in the procedure.	Richard Cockerill Digital Forensics Manager December 2015	
6	For the initial scoring of MPU examinations to be undertaken, to ascertain their priority level and ensure the log of outstanding examinations is regularly monitored and reviewed as continued good practice.	Merits Attention	The volume of mobile phone submissions makes compliance with the HTCUC matrix untenable under current resourcing arrangements. All submissions which relate to Indecent Images of Children are required to be submitted to HQ and these will now be subject to HTCUC processes. Those cases identified as urgent, such as Major Crime Enquiries, will continue to be prioritised on a case by case basis. Volume crime will continue to be managed by investigation hub supervisors in line with their competing demands.	Richard Cockerill Digital Forensics Manager July 2016	
7	Current procedure should be updated to include the requirement for the FSD9 submission form and Digital Media Examination to be scanned on to the Niche record of an occurrence.	Merits Attention	Richard Cockerill will circulate this requirement and include it within updated procedures under 17025.	Richard Cockerill Digital Forensics Manager July 2016	

NOT PROTECTIVELY MARKED

Final

8	Detective Inspectors should be appropriately reminded of the need to complete the SNC spreadsheet for mobile phone examinations, liaising with OIC and District examiner where further detail may be needed.	Merits Attention	The updated procedures and Niche requirements will negate the need for the spreadsheet to be maintained in the medium to long term.	Richard Cockerill Digital Forensics Manager July 2016	
---	--	------------------	---	--	--

5 Recommendations

6: Appendix: Assurance Level

Internal Audit assesses the effectiveness of internal control, within the scope of what is audited. This measure is therefore a relative one.

Classification of Recommendations	
Fundamental	Action is needed to address risks that could impact on the organisation's ability to achieve its objectives. Action will typically be organisation-wide and be necessary at the highest level. Other fundamental recommendations will be made in regard to potentially serious breaches of statutory obligations.
Significant	Action is needed to address risks that impact primarily on one major business area or to address lower risks on an organisation-wide basis.
Merits Attention	Action is advised to enhance control, remedy minor breaches of current controls or to improve efficiency.

Category	Description
1	Reasonable assurance can be provided that the main risks considered are being effectively managed; action may still enhance the management of risk in a small number of areas. In addition Internal Audit has identified that the approach taken to address risk as representing good practice in this area.
2	Reasonable assurance can be provided that the main risks considered are being effectively managed. Limited management action may be required to address a small number of significant issues.
3	Limited assurance can be provided that the main risks considered are all being effectively managed. Significant management action is required to address some important weaknesses.
4	Inadequate assurance can be provided that the risks identified are being effectively managed. Significant weaknesses have been identified in the risk management action, these are likely to involve major and prolonged intervention by management. These weaknesses are such that the objectives in this area are unlikely to be met.

7 Appendix: Overall Assessment Criteria

Risks in this report have been assessed using the following criteria. It is the same criteria as that used by North Yorkshire Police to assess risk for the Risk Register.

Probability	Highly Probable	Nil	5:7	4:12	2:14	1:16
	Probable	Nil	5:4	5:8	3:13	2:15
	Unlikely	Nil	6:2	5:5	5:10	4:11
	Highly Improbable	Nil	6:1	6:3	5:6	5:9
	Nil	Nil	Nil	Nil	Nil	Nil
		Nil	Negligible	Minor	Significant	Catastrophic
Impact						

Probability	Nil	< 20% Highly Improbably (HI)	20% - 40% Unlikely (UL)	40% - 60% Probable (P)	> 60% Highly Probable (HP)
Impact Categories	Nil	Negligible	Minor	Significant	Severe
Financial (£) - Default - Mandatory	Nil	0 => 100k Increased financial impact less than £100000	100k => 250k Increased financial impact between £100k and £250k	250k => 2.5m Increased financial impact between £250k and £2.5m	2.5m => 3.75m Increased financial impact greater than £2.5m
Reputation	Nil	Negligible adverse publicity. Minimal impact upon public perception	Localised adverse publicity. Minor/transient impact upon public perception of Force or PCC	Criticism at local level. Lasting impact upon public perception of Force or PCC	Intense national media. Criticism at national level
Operational	Nil	Negligible impact upon ability to deliver service and meet Force targets	Minor impact upon ability to deliver service and meet Force targets	Significant impact upon ability to deliver service and meet Force targets	Catastrophic impact upon ability to deliver service and meet Force targets
Legal/Compliance	Nil	Negligible prospect of legal challenge	Minor/Transient prospect of legal challenge	Serious non-compliance. Litigation/challenge.	National legal issue.