Protective Marking	*Not Protectively Marked*
Suitable for Publication Scheme? Y/N	Y
Title & Version	Self-Self Equipment Kiosk Local Working Instructions V1.1
Relevant	All Officers and Staff including SSE Kiosk examiners and DCC staff
Author	1 [redacted]
Authorised by	[redacted]
Creating Branch Code and Operational Command Unit/Directorate	Digital Cyber & Communications (DCC), Forensic Services
Summary/Purpose	The purpose of this document is to provide a Local Working Instructions (LWI) for Police Officers and SSE kiosk users when submitting digital devices for SSE kiosk forensic examinations
Date Issued	
Review Date	
IF PRINTED OUT THIS IS NOT A CONTROLLED DOCUMENT	

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised by
1.0	**11/01/2016**	**First Draft**	2 [redacted]
1.1	**01/03/2016**	**Amendment**	

Table of contents

1. Purpose

1.1 This guidance document describes the process for the lawful examination of digital devices[1], seized during the course of and an investigation using the Digital, Cyber and Communications (DCC) Self-Service Equipment (SSE), also know as Digital Forensic Kiosks (DFKs). This document outlines the following:

- The submission process for digital devices for SSE kiosk forensic examination (LEVEL 1); **HOW** and **WHEN** to escalate to a Level 2 (Digital Hub) or/and Level 3 (DCC Central Laboratory) forensic examination for digital devices (see Figure 1 and 1.1 refers)
- Best practice to be adopted to around the seizure of digital devices requiring forensic examination
- Guidance to Police Officers and SSE kiosk examiners on actions to be taken on completion of a SSE kiosk forensic examination

1.2 In addition to the above, this Local Working Instruction (LWI) will enable a consistent and lawful method of processing the personal data obtained from digital devices during the course of and investigation. This LWI aims to ensure our processes are compliant with our obligations under legislation such as Criminal Procedures and Investigation Act 1996 (CPIA), Data Protection Act 1998 (DPA), Human Rights Act 1998 (HRA) and also the Management of Police Information Code of practice 2010 (MOPI).

2. Introduction and Current Position

2.1 The SSEs[2] are located through out the Boroughs within the Metropolitan Police boundaries. Each SSE will have a nominated Single Point of Contact (SPOC). The SPOC will assist the DCC, Forensic Services, in the management and compliance of the SSE facilities, those activities will include:

- Location of SSEs and logistical support (e.g. access to an Aware, printer and phone)
- Provision of secure exhibits storage
- Point of liaison between DCC and accredited SSE kiosk users
- Ensure that provisions are in place around consumables (e.g. DVDs/CDs Exhibit bags, Hazard tape, fingerprint do not touch labels)
- Establishing a process for alerting SSE accredited kiosk users when exhibits require examination
- Establishing a process with other triage SSE SPOC colleagues to manage shared SSE facilities
- Maintenance and publication of list of trained SSE examiners
- Review of SSE accredited kiosk user compliance and provide escalation, if required; between DCC management team and operational policing

[1] Mobile devices, media cards/USB sticks, SIM cards, Satellite Navigation Systems, Tablet devices
[2] Currently 50 kiosks, to be increased to 90 SSE kiosks by 2016-17

2.2 Details of accredited SSE kiosk examiners can be found by contacting local SPOCs, DCC digital hubs or and the DCC Website.[3]

3. Scope & Environment

3.1 Whereby digital devices are seized during the course of an investigation the capability is available to conduct a forensic examination using the SSE kiosks by trained and accredited kiosk users. SSE kiosks must not be used for the examination of exhibits seized during covert investigations, when there may be legal, journalistic or confidential personal information on the device. **If in doubt seek advice form the one of the DCC digital hubs or DCC central laboratory**.

3.2 Submitting directly to DCC digital hub or DCC central laboratory
Submission of exhibits directly for a level 2 or/and level 3 forensic examination will be accepted in cases where:

1). The exhibits for examination are contaminated with biological/chemical hazards (warning labels should be clearly visible on packaging)

2). Voicemail is required

3) Digital device has been attempted on the SSE kiosk, and is not supported, or the acquisition of data has not been successful on the SSE kiosk

4). Examination has been attempted on the SSE kiosk and additional specialist examination is required

5). Following a charging decision where a not guilty plea is entered, an exhibit requires further evidential analysis if the SSE kiosk evidential product (i.e. the SSE kiosk examiner, OIC statements and exhibited report/section of the report) is relevant and disputed

6). When it is **KNOWN** that the device is security locked upon seizure, and unlocking is not supported by the SSE kiosk, can be escalated to DCC digital hub or DCC central laboratory. If a device is known to be security locked upon seizure the OIC can still submit the media card and SIM Card, if fitted, for a SSE kiosk examination; as this may provide sufficient evidence/intelligence for the purposes of that investigation, even though the device may be security locked

3.3 If unsure what level of forensic examination a submission is required then contact your local DCC digital hub who will be able to advise on the best course of action in relation to digital submissions.

[3] http://intranet.aware.mps/SC/Forensics/OCU_Sites/DEFS/Self+Service+Equipment+%28SSE%2c+also+called+Digital+Forensic+Kiosks%29.htm

4. Application and Responsibilities

4.1 Ownership of LWI: 3

4.2 Implementing LWI: All police officers and staff including SSE examiners and DCC and Forensic Services staff.

4.3 Approving the LWI: 4 Head of DCC.

4.4 Review Date: 12 Months

5. Lawfully Obtaining Digitally Held Data

5.1 Officers and staff are reminded that only data contained within the device is retrievable using PACE. Any additional actions undertaken by officers or staff to obtain data held on servers or platforms that may be accessible using the device will be treated as unauthorised unlawful access and will be formally investigated. This will include voicemail that has not been pushed to the device and held in an audio file where the required legislation and or consent has not been obtained prior to access. It is, therefore, important that officers and staff follow this guidance fully and refer to DCC for further guidance or specialist advice.

5.2 The lawful process in obtaining digitally held data from personal devices slightly differs depending upon the investigative status of the subject.
Suspects: An officer can exercise his/her powers under PACE in obtaining material which is relevant to an investigation.

Victims and Witness: Where a device has been provided to police, either by a victim or witness, in order to identify data that may be relevant to an investigation or evidence of an offence the ***Form 107*** (found on the forms website) must be completed and "explicit consent" obtained prior to the examination taking place.

5.3 Where consent is not provided, and the investigation necessitates the need for the MPS to access certain information held on that device (in order to prevent or detect a crime or apprehend an offender), an officer may consider exercising his / her powers to obtain the required information. In such circumstances, full justifications must be recorded on the CRIS system. Where a legitimate power does not exist, the officer will not, under and circumstances, attempt to obtain material from the device in question.

5.4 In cases where the acquisition of data from the device fails and the device has to be submitted or escalated then a copy of the Form 107 must accompany the submission to ensure that data is not acquired if consent has not been given to its acquisition.

If consent has not been given, and the officer has exercised their discretion under their statutory powers to seize the device, this explanation should accompany the submission of the device if escalated from a Level 1 type examination to a Level 2 or/and 3 type examination.

6. Seizure & Packaging

6.1 **Seizure:**

When recovering a mobile device where a forensic examination is required, seizing officers, where practical are use to use the ***Form 106***, which is available via forms on the internet. The form provides full guidance in relation to the seizure and correct packaging of mobile devices for the packaging of mobile devices for forensic examination; it includes provision around DNA and Fingerprint presentation.

6.2 **Packaging:**

The integrity around packaging of exhibits, is based around the acceptance of risk, but **ANY** submission that could involve dual examination **MUST** be boxed to give the best chance of maintaining the forensic integrity of the device for fingerprints or/and DNA.

7. SSE submission process overview for Officers using Level 1 Service

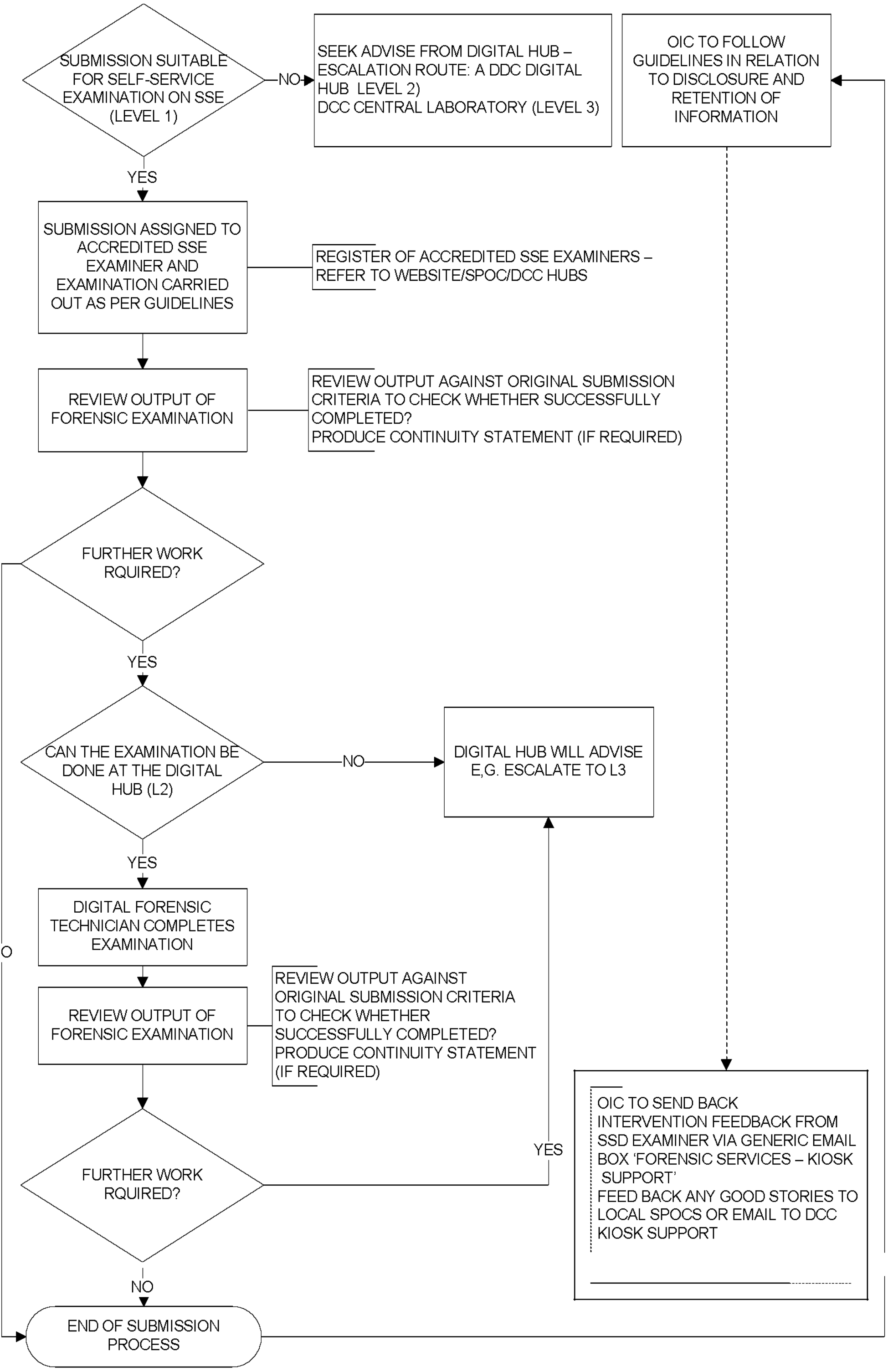

SUBMISSION SUITABLE FOR SELF-SERVICE EXAMINATION ON SSE (LEVEL 1)
NO
SEEK ADVISE FROM DIGITAL HUB – ESCALATION ROUTE: A DDC DIGITAL HUB LEVEL 2) DCC CENTRAL LABORATORY (LEVEL 3)
OIC TO FOLLOW GUIDELINES IN RELATION TO DISCLOSURE AND RETENTION OF INFORMATION
YES
SUBMISSION ASSIGNED TO ACCREDITED SSE EXAMINER AND EXAMINATION CARRIED OUT AS PER GUIDELINES
REGISTER OF ACCREDITED SSE EXAMINERS – REFER TO WEBSITE/SPOC/DCC HUBS
REVIEW OUTPUT OF FORENSIC EXAMINATION
REVIEW OUTPUT AGAINST ORIGINAL SUBMISSION CRITERIA TO CHECK WHETHER SUCCESSFULLY COMPLETED?
PRODUCE CONTINUITY STATEMENT (IF REQUIRED)
FURTHER WORK RQUIRED?
YES
CAN THE EXAMINATION BE DONE AT THE DIGITAL HUB (L2)
NO
DIGITAL HUB WILL ADVISE E,G. ESCALATE TO L3
YES
DIGITAL FORENSIC TECHNICIAN COMPLETES EXAMINATION
NO
REVIEW OUTPUT OF FORENSIC EXAMINATION
REVIEW OUTPUT AGAINST ORIGINAL SUBMISSION CRITERIA TO CHECK WHETHER SUCCESSFULLY COMPLETED?
PRODUCE CONTINUITY STATEMENT (IF REQUIRED)
OIC TO SEND BACK INTERVENTION FEEDBACK FROM SSD EXAMINER VIA GENERIC EMAIL BOX 'FORENSIC SERVICES – KIOSK SUPPORT'
FEED BACK ANY GOOD STORIES TO LOCAL SPOCS OR EMAIL TO DCC KIOSK SUPPORT
YES
FURTHER WORK RQUIRED?
NO
END OF SUBMISSION PROCESS

Figure 1. Overview of submission process for Officers submitting to Level 1 service (SSE)

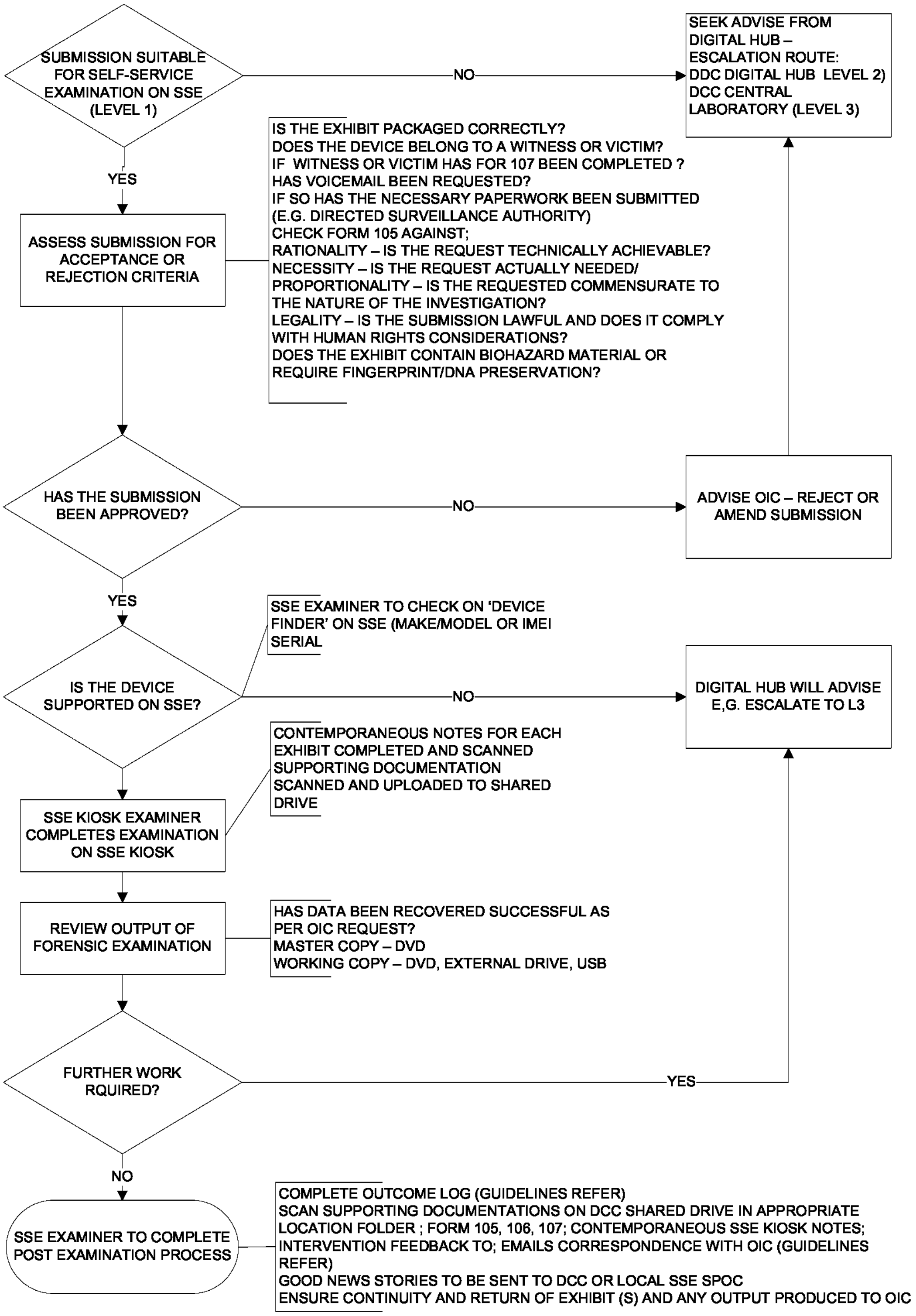

SUBMISSION SUITABLE FOR SELF-SERVICE EXAMINATION ON SSE (LEVEL 1)
NO
SEEK ADVISE FROM DIGITAL HUB – ESCALATION ROUTE: DDC DIGITAL HUB LEVEL 2) DCC CENTRAL LABORATORY (LEVEL 3)
YES
ASSESS SUBMISSION FOR ACCEPTANCE OR REJECTION CRITERIA
IS THE EXHIBIT PACKAGED CORRECTLY?
DOES THE DEVICE BELONG TO A WITNESS OR VICTIM?
IF WITNESS OR VICTIM HAS FOR 107 BEEN COMPLETED ?
HAS VOICEMAIL BEEN REQUESTED?
IF SO HAS THE NECESSARY PAPERWORK BEEN SUBMITTED (E.G. DIRECTED SURVEILLANCE AUTHORITY)
CHECK FORM 105 AGAINST;
RATIONALITY – IS THE REQUEST TECHNICALLY ACHIEVABLE?
NECESSITY – IS THE REQUEST ACTUALLY NEEDED/
PROPORTIONALITY – IS THE REQUESTED COMMENSURATE TO THE NATURE OF THE INVESTIGATION?
LEGALITY – IS THE SUBMISSION LAWFUL AND DOES IT COMPLY WITH HUMAN RIGHTS CONSIDERATIONS?
DOES THE EXHIBIT CONTAIN BIOHAZARD MATERIAL OR REQUIRE FINGERPRINT/DNA PRESERVATION?
HAS THE SUBMISSION BEEN APPROVED?
NO
ADVISE OIC – REJECT OR AMEND SUBMISSION
YES
SSE EXAMINER TO CHECK ON 'DEVICE FINDER' ON SSE (MAKE/MODEL OR IMEI SERIAL
IS THE DEVICE SUPPORTED ON SSE?
NO
DIGITAL HUB WILL ADVISE E,G. ESCALATE TO L3
CONTEMPORANEOUS NOTES FOR EACH EXHIBIT COMPLETED AND SCANNED SUPPORTING DOCUMENTATION SCANNED AND UPLOADED TO SHARED DRIVE
SSE KIOSK EXAMINER COMPLETES EXAMINATION ON SSE KIOSK
REVIEW OUTPUT OF FORENSIC EXAMINATION
HAS DATA BEEN RECOVERED SUCCESSFUL AS PER OIC REQUEST?
MASTER COPY – DVD
WORKING COPY – DVD, EXTERNAL DRIVE, USB
FURTHER WORK RQUIRED?
YES
NO
SSE EXAMINER TO COMPLETE POST EXAMINATION PROCESS
COMPLETE OUTCOME LOG (GUIDELINES REFER)
SCAN SUPPORTING DOCUMENTATIONS ON DCC SHARED DRIVE IN APPROPRIATE LOCATION FOLDER ; FORM 105, 106, 107; CONTEMPORANEOUS SSE KIOSK NOTES; INTERVENTION FEEDBACK TO; EMAILS CORRESPONDENCE WITH OIC (GUIDELINES REFER)
GOOD NEWS STORIES TO BE SENT TO DCC OR LOCAL SSE SPOC
ENSURE CONTINUITY AND RETURN OF EXHIBIT (S) AND ANY OUTPUT PRODUCED TO OIC

Figure 1.2 Overview of SSE submission (Guidance for SSE kiosk examiner

7.1 Figures 1.1 and Figure 1.2 is a generic overview of the submission process, and provides guidance and considerations for both the submitting officer and SSE kiosk examiner when submitting a digital device for a forensic examination. A detailed description of some of those submission processes are covered in this guidance document.

7.2 Throughout the submission process communication between the investigating officer and the SSE kiosk examiner should be encourages so that resources and time are managed effectively and decisions managed to avoid delays to the investigation and to achieve the best possible outcome.

8. Considerations when submitting for a Level 1 (SSE), Level 2 (Digital Hubs), Level 3 (Central Laboratory)

8.1 Where practical and supported, in the first instance, the investigating officer is to use the SSE kiosk facility for the forensic examination of digital devices (where not reference back to Paragraph 2 of this document).

8.2 DCC Digital hubs can be tasked direct, however they will prioritise on a case by case basis, whether SCO or TP Tasking, submission criteria will be based on:

- Life at risk
- Those submissions whereby the suspect or suspects are in custody and the examination will assist a charging decision
- Those submissions whereby vulnerable witness and/or victims have been identified
- Those submissions which involve a short bail to return timescale and the examination will assist in a charging decision or assist in the investigation
- Those submissions whereby data (such as CCTV footage) will be lost or it time sensitive
- Those submissions whereby data is required for court with very short timescales

8.2 There will be circumstances whereby a submission may not be suitable for a Level 1 type examination using the SSE kiosk; some of those reasons are listed below:

Security locked devices
If the OIC is unable to obtain the handset security code from the owner/user and there is still a requirement for this exhibit to be examined, the triage process is as follows:

- Through the 'Device Finder' application available on the SSE kiosk; searches of supported makes and model of mobile devices and applications can be made and also provides information whether a particular digital device can be 'unlocked' by the SSE kiosk
- Where practicable, seek advice from one of the digital hubs, it may be that the device can be submitted directly to the digital hub or escalated to DCC central laboratory

Not Supported by Digital Hub
The examination cannot be completed using the forensic tools available at the digital hub.

Specialist Examination (further work required)
If review of the report generated from either the kiosk or/and the DDC digital hub forensic examination identifies specific data requested (e.g. non standard messaging application or media files) that has not been acquired by those processes, and this information is still is required to support the investigation can be escalated by the investigation officer to the DCC central laboratory. The exhibit can be submitted to DCC central laboratory for specialist examination using the eMGFSP submission process. Advice from the digital hub should be included in the submission and will be subject to a further assessment for proportionality and rationality. If the exhibit is being submitted for potential deleted SMS messages the OIC is advised that this request must be supported by itemised billing data from the CIU (Communications Intelligence Unit).

Specific Evidential Analysis
If, following the charging decision the defendant enters a plea of not guilty and the digital forensic evidence obtained at the kiosk or digit hub is disputed, the exhibit will require submission the DCC central laboratory for specific analysis to address the issues in dispute. A submission should be made via the eMGFSP submission process. All work undertaken by either the kiosk or/and DCC digital hub in association with the disputed exhibit should be submitted along with the eMGFSP request.

Illicit Images of Children (IIoC) Submissions
Due diligence should be carried out by both the investigating officer and the SSE kiosk examiner to Illicit Images of children (IIoC) being discovered during the forensic examination process. The SSE Kiosks can be used for IIoC submissions; however, the device (s) may need to be escalated to DCC using the eMGSFP submission process[4] whereby advance extraction or/and provenance may be required.

The SSE kiosk has encryption enabled, whereby the extraction process and subsequent output from the SSE kiosk is protected and can only be viewed or access with a password The SSE kiosk examiner also has the ability to exclude the extraction of specific data-sets during the course of a forensic examination and only filter[5] out the information as specified or requested in the submitted documentation. **On NO circumstances is IIoC material to be viewed on the AWARE system.**

8.2 If a submission involves a large number of devices, or/and is complex in nature, or/and is an ongoing investigation then the investigation officer should seek guidance and advice from the regional ***Digital Strategy Advisor (DSA)***. The DSA can advise upon a digital forensic strategy to identify and maximise opportunities, obtaining best evidence, assist in the coordination and allocation of resources to that investigation.

[4] If SSE kiosk has been used, then examination references and exhibit produced should be included
[5] Sub reporting, only exporting information whereby consent has been obtain (Form 107)

8.3 Whereby a submission has already been undertaken by a digital hub, any escalation to the DCC central laboratory e.g. whereby additional work has been agreed, the process will be managed by the digital hub in consultation with the investigating officer and DCC staff.

9. Submission process - guidance for Police Officers and SSE examiners

9.1 Submission to the SSE kiosk will be via a ***Form 105,*** the submission process to the DCC digital hub and DCC central laboratory will be via a Form 105 or **eMGFSP**[6] depending on the forensic service requested.

9.2 Both the eMGFSP and Form 105 process requires the investigating officer to document the rationale for the specific information required form the device to assist in the investigation, giving due consideration to the proportionality and legality of the request.

9.3 The eMGFSP is the main forensic submission form that is submitted trough the Goddard system. The Form 105 was a form used for the Territorial Policing mobile phone examination project and is now used to undertake forensic examinations on the SSE kiosk. Both methods of submission will be used in the medium term until the delivery of a new case management system.

9.4 Where voicemail retrieval has been requested and the exhibit belongs to a victim, 'explicit consent' has to be obtained prior to the examination taking place. In other circumstances 'directed surveillance authority' has to be obtained prior to the examination taking place.

9.5 If the exhibit has been seized from a suspect or defendant then the investigating officer must provide a custody or CAD reference for that exhibit sized: failure to provide this information will result in the submission being rejected.

9.6 **Rejected Submissions:**

A SSE kiosk examiner will reject examination requests where the following requirements are not met:

- Exhibits have not been packaged in accordance with best practice
- Relevant information has not been provided on the request form

If a submission is rejected by the SSE kiosk examiner the investigating officer will be notified by the kiosk examiner. The reason for rejection will be documented on the request form, the Book 105 updated and the exhibits returned to the OIC/secure storage.

It is the responsibility of the investigating officer to address the reason for rejection (e.g. not proportionate or rational provided in reasons for request) and re-submit the request. If necessary a new TP Phone Examination Request form 105 will need to be completed for the resubmission.

[6] Computer examinations -eMGFSP only; Phone examinations Form 105 & eMGFSP; CCTV.Video Form 105 & eMGSFP

9.7 Terminated Examinations

It may be necessary for the SSE kiosk examiner to terminate the examination during the process. Examinations may be terminated for the following reasons:

Locked Handsets

The examination process may reveal the exhibit is PIN or handset locked. If PIN or handset security codes are not recorded on the request form, the examiner will not be able to proceed with the examination. Examination of the exhibit will be terminated, the Book 105 updated and the exhibit returned to the OIC/secure storage. The kiosk examiner will notify the OIC and complete the relevant PIN/PUK or Handset Lock information request form.

It is the responsibility of the OIC to request the PIN information from the owner/user or, if unavailable, the PUK information from the CIU.

On receipt of the PIN or PUK code the OIC must update the request form and resubmit the exhibit for examination. It is the responsibility of the OIC to obtain any handset security codes from the owner in the first instance. If the OIC is unable to obtain the handset security code from the owner and there is still a requirement for the exhibit to be examined it can be submitted to DCC using the eMGFSP submission process.

Non-supported Handsets;

There may be occasion where an exhibit submitted for examination is not able to be examined using the SSE kiosk. If an examination is not supported by the SSE kiosk the process will be terminated and escalated to one of the regional DCC digital hub central. The Book 105 should be updated and the exhibit returned to the OIC/secure storage. The kiosk examiner will notify the OIC.

C. Illicit Images of Children:

The SSE Kiosk can be used for Illicit Images of children (IIoC) submissions; however, where a submission is not related to IIoC, due diligence should be carried out by both the OIC and the Kiosk examiner to IIoC being discovered during the forensic examination process. The SSE kiosk examiner has the option to terminate the process, sub-report without exporting the IIoC media. If exported the SSE kiosk examiner is to follow local policy around IIoC and return the original exhibit to the OIC. Please note that the SSE Kiosk will only do a logical[7] only extractions, so if deleted data or further provenance is required a further submission can be made to DCC using the eMGFSP process.

9.8 Completed Examinations:

The examination output from each exhibit using a SSE kiosk will be produced a Master Copy output. A Working Copy can be exported on different storage media including, USB media and external storage on the SSE kiosk.

The Master Copy is the SSE kiosk examiners exhibit and will be sealed and exhibited (local policy applies) and returned to the OIC on completion of the forensic examination. The master copy must be retained for disclosure in the event it is required by a defence expert.

[7] Logical refers to data which may viewed or stored on the device - does not include deleted data

The working copy will be and returned to the OIC and can contain the following formats:

- PDF File - data extracted presented in a report format, for use by OIC.
- XRY MSAB encrypted Output[8]
- Excel Output
- MSAB Viewer (which the allows the content to be viewed in a reportable format)

If the SSE kiosk XRY container is exported (both within the Master and Working copy), will contain an executable SSE kiosk 'viewer' application that allows the user of the end product to view the information as seen on the SSE kiosk. The end user has the ability to produce sub-reports from the original data extracted by the SSE kiosk examiner.

9.9 On completion of the examination process the SSE kiosk examiner will notify the OIC. Processes and procedures around continuity of the original exhibit and any exhibits produced will be down to the local policy of the SSE kiosk location.[9]

10. Data Retention - Guidance for Police Officers and SSE kiosk examiners

10.1 **Retention or destruction**
During the investigative or trial process the data will be reviewed in order to ascertain if it should be retained in furtherance of our policing purposes. Such examples can include the following:

- The purpose of further reviews or future investigations
- Judicial reviews or other civil litigation
- CPIA, MOPI, and DPA compliance
- Intelligence

10.2 Where data is considered to have no policing purpose then the organisation has a statutory obligation to delete that data. It is acknowledged that the manner in which data is acquired and delivered to investigators may make the division of individual files or data strings within the acquired data impossible to separate into irrelevant and relevant material. However, where the entire file has been considered and a decision is made that the material has no investigative, intelligence or evidential value then it must be deleted, in line with the METSEC Code, the 'Information Considerations when Repairing, Re-using or Disposing of ICT Equipment and ICT Storage Media SOP, and the MPS Review, Retention and Disposal Schedule within the MPS Records Management Manual.

10.3 It is recommended that a succinct but clear note relating to the retention or destruction of digital material is placed within the CRIS report outlining the rationale for retention or destruction of the material obtained

[8] XRY MSAB output is an encrypted container which contains the acquisition photos taken during the forensic examination and selected output files of the extraction of the digital device - the container can only be opened with a password as generated by the SSE kiosk examiner who undertook the forensic examination

[9] Continuity around securing, booking-in and out of exhibits will be down to local policies as implemented by the SSE kiosk SPOC

10.4 Handling Irrelevant Data

When a SSE kiosk is used to obtain electronic data from a mobile device, it will obtain all data of a particular type, rather than just the individual data that is relevant to a particular investigation. For example, if a photograph on a 'witness' mobile phone is relevant, because it shows an offence being committed, then the kiosk will acquire all photographs on that phone, rather than just the photographs of the offence. If text messages to a victim of harassment are required to investigate the harassment allegations, then kiosk will acquire all text messages on that phone, rather than just the relevant individual messages or text conversations. This collateral irrelevant data is inextricably linked to relevant data at the time it is obtained. As much of this collateral irrelevant data will amount to personal data of the victims, witnesses and suspects that it was obtained from, the MPS must ensure that working practices do not infringe on the privacy rights of the individuals whom the data was obtained from. Those rights are protected by the Human Rights Act 1998 and the Data Protection Act 1998.

The following paragraphs set out the requirements for dealing with this type of collateral irrelevant inextricably linked data:

- When a SSE kiosk is used to acquire data from a mobile device, a copy of that data will be stored as an exhibit copy on a CD/DVD and another copy will be stored as a working copy on a storage media
- As the exhibit will only be accessed and used to establish the provenance of the evidence contained on it, there is only a minimal engagement of the right to privacy in respect of any collateral data contained on that exhibit CD. That minimal engagement of the right to privacy will not amount to a breach of the HRA or DPA because it is necessary to prove the integrity of the evidence obtained from the mobile device
- The working copy of the master copy is where the most care must be taken. Whilst irrelevant data may be inextricably linked to relevant evidence, it is likely that it will be possible to separate the collateral irrelevant data from the data that is considered to be relevant. This will enable the investigator to review and delete information during / at the conclusion of the investigative / or judicial process
- This process will allow the organisation to avoid inadvertently breaching the HRA and DPA because irrelevant personal data that can be, will be separated from other material and appropriately dealt with at the earliest possible stage

11. Disc Handling and Using Reports

11.1 Creation of Discs

Following a successful forensic examination on a SSE kiosk, the default option for the SSE kiosk when exported a Master Copy will always be a disc. The Working Copy can be disc, USB thumb drive or external storage.

The Master copy is the Examiners exhibit and should be exhibited by the SSE kiosk examiners using the following naming conversion (See figures 2.1 and 2.2 example of naming convention). Both Master and Working copies should be labelled with the following details:

- RESTRICTED (if applicable)
- CRIS reference number (or custody if no CRIS available at time of examination)
- Disc exhibit reference your initials/unique identifier (e.g. EJF/1)
- Note of original exhibit examined to denote where the information came from and a brief description of what is contained on the recorded media (e.g. handset reports)

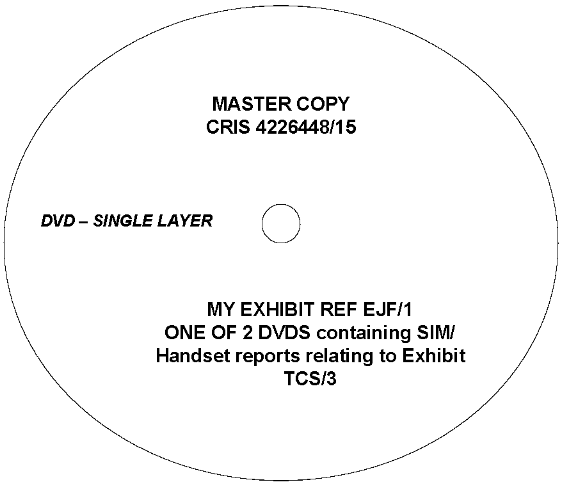


Figure 2.1 Naming convention of CD/DVD Master Copy

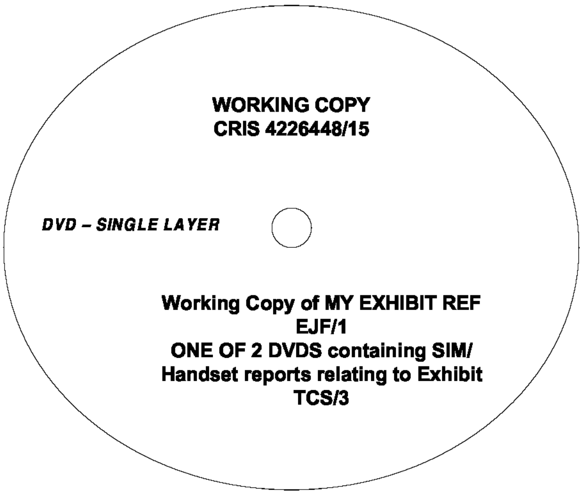

WORKING COPY
CRIS 4226448/15
DVD – SINGLE LAYER
Working Copy of MY EXHIBIT REF
EJF/1
ONE OF 2 DVDS containing SIM/
Handset reports relating to Exhibit
TCS/3

Figure 2.2 Naming convention of CD/DVD Working Copy

The Master copy should be labelled. Sealed in an evidence bag the SSE contemporaneous notes updated. The working copy should be labelled and placed in a protective cover and the SSE contemporaneous notes updated.

Both the Master and Working copy of the discs should be handed to the OIC along with the original exhibits. The discs should be entered into the Book 105 as one new entry. The 105 reference for the discs should be cross referenced in the Book 105 under related 105 entry column in order the OIC can identify his/her relevant discs. It is suggested the sealed and exhibited discs are placed in an unsealed bag with the original exhibits to keep the submission together. Update your notes with the disc exhibit 105 reference numbers.

11.2 **Disc handling and storage of information**

On receipt of the Master Copy must be retained for the purpose of Integrity, continuity and disclosure in the event it is required by a defence expert or/and the material is reasonably challenged and/or disputed. The content of the working copy10 can be reviewed by the investigating officer to establish the relevance of any data to the investigation. **UNDER NO CIRCUMSTANCES SHOULD FILES, EXERTS OR COPIES OF FILES FROM THE MEDIA EXPORT BE SAVED TO PERSONAL FOLDERS ON THE AWARE SYSTEM**. Reports generated from the Kiosk output will be stored on a designated folder as dictated by local policy and access rights for the OIC to review specific case data will be the responsibility of the designated Information Managers[11]. Officers should contact their Information Managers to arrange creation of and access to the shared drive folder[12]. Any documents[13] created by the OIC in the course of the investigation e.g. exerts of reports from the original output, **must be stored within this shared drive**.

11.3 If there is a requirement for the data to be stored 'out of Information Managers office hours' (e.g. where an exert of the report is required for an urgent charging decision) then it may be ***temporarily stored*** by the OIC to a personal folder. The OIC MUST, at the same time email the Information Manager requesting shared folder creation and access. On notification from the IM that the shared folder is created, the OIC **MUST IMMEDIATLEY** files all the documents into the shared folder and deletes the copy stored in the personal folder. It is the responsibility of the OIC to adhere to this lawful order. Once the data has been copied to from the disc to the shared drive, it should be retained in accordance with the MPS Review, Retention and Disposal Schedule within the MPS Records Management Manual.

11.4 **Using reports**

Content of the report can be used during the interview process, submitted to support a charging decision and used as evidence when accompanied by a statement from the kiosk examiner and investigating officer. Information produced from the working copy output (printed report or exerts from a report) will be the investigating officers' exhibit. Kiosk examiners will produce a pro forma statement detailing their actions as part of the examination process. This statement will be made available to the OIC, along with the Master and Working Copy, and original exhibits

.

[10] Working Copy can be exported onto a CD/DVD, USB Thumb-Drive

[11] Information Managers or designated IM personnel

[12] Shared drive - local policy applies

[13] The Kiosk report output can be XCEL, PDF or MSAB encrypted file container

Interview: The report /exerts of the report can be used during the interview process. A copy of the report/ extract of relevant data from the report should be exhibited by the investigating officer (OIC).

Charging Decision: The investigating Officer can produce a commentary style statement (as per CCTV) to evidence the relevant data from the kiosk generated report. The investigators officers' commentary statement supported by the relevant printed and exhibited sections/pages of the kiosk generated report can be submitted with the kiosk examiners statement as part of the case papers for a charging decision.

PCMH or first hearing: Following a charging decision where a not guilty plea is and the digital forensic evidence is relevant and disputed, it will be necessary to submit the exhibit to DCC for further evidential analysis by a Forensic Engineer to address the areas of dispute.

IMEI and NMPR: The report will contain the detail of the IMEI number. If appropriate this information should be used to check against the National Mobile Property Register as per existing Borough processes.

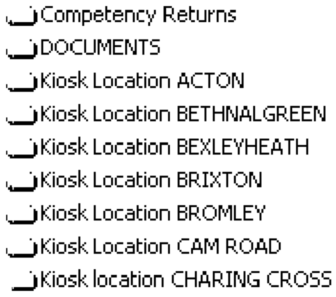
12. Post examination processes - Guidance for Officers and SSE users

12.1 Post examination processes have been put in place to assist in the capturing of 'key' information on how this end product generated from an SSE kiosk is being used in an investigation. This information allows us to evaluate the effectiveness of the SSE kiosks and supports the ongoing business case for the self-service examination of digital devices.

12.2 **Updating Location Databases - SSE kiosk examiners**
On completion of a competency assessment SSE accredit kiosk examiners are given access to a DCC shared location on AWARE[14]. It is the responsibility of the SSE kiosk examiner to ensure that ALL documentation[15] in relation to the submission e.g. contemporaneous notes, intervention feedback form and email correspondence is either scanned or exported into the generated CRIS folder by the SSE kiosk examiner. Figure 2 to 2.3 show the folder structure in the shared drive:

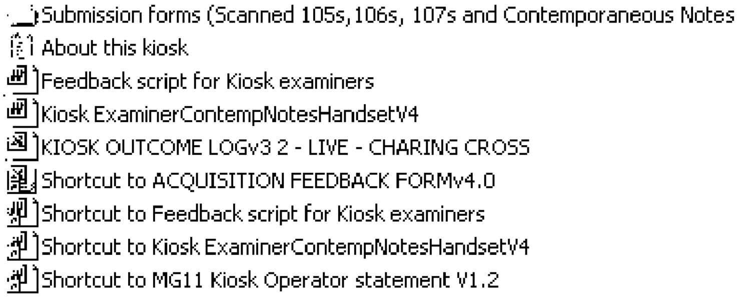
[14] S:\All HQ Departments\Directorate of Information\DEFS Data\Reports\KIOSKS - LEVEL 1\USERS

[15] Forms 105, 106, and 107; SSE Contemporaneous notes for each exhibit; email correspondence between the OIC and the SSE kiosk examiner who conducted the forensic examination



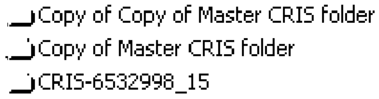
Competency Returns
DOCUMENTS
Kiosk Location ACTON
Kiosk Location BETHNALGREEN
Kiosk Location BEXLEYHEATH
Kiosk Location BRIXTON
Kiosk Location BROMLEY
Kiosk Location CAM ROAD
Kiosk location CHARING CROSS

(Fig 3.0: Each location with an SSE kiosk will have a folder generated)



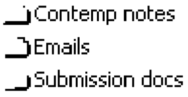
Submission forms (Scanned 105s,106s, 107s and Contemporaneous Notes
About this kiosk
Feedback script for Kiosk examiners
Kiosk ExaminerContempNotesHandsetV4
KIOSK OUTCOME LOGv3 2 - LIVE - CHARING CROSS
Shortcut to ACQUISITION FEEDBACK FORMv4.0
Shortcut to Feedback script for Kiosk examiners
Shortcut to Kiosk ExaminerContempNotesHandsetV4
Shortcut to MG11 Kiosk Operator statement V1.2

(Fig 3.1; showing Sub-folders contained in each individual location folder)



Copy of Copy of Master CRIS folder
Copy of Master CRIS folder
CRIS-6532998_15

(Fig 3.2. showing Sub-folders contained in Submission Forms folder)



Contemp notes
Emails
Submission docs

(Fig 3.3. showing individual folders contained in the template Master CRIS folder)

12.3 **SSE kiosk location Outcome Log**
Each SSE kiosk will have an Outcome excel spreadsheet for each location, where there are multiple SSE kiosks in one location then only one location outcome log will exist.

12.4 It is the responsibility of the SSE kiosk examiner to ensure that the relevant columns are recorded and updated for each exhibit where an SSE kiosk has been used. ***Appendix A*** to this guidance document shows an example of an outcome log, guidance which columns in the excel spreadsheet are to be completed by the SSE kiosk examiner. The SSE kiosk examiners are reminded that the majority of these columns are dropdowns e.g. crime types, and free text should not be used where these dropdowns are available.

12.5 Compliance in ensuring that the outcome logs are competed correctly will be the responsibility of the nominated SPOC for either TP or SCO for that assigned SSE kiosk examiner.

12.6 **SSE Acquisition feedback Form**
On completion of a successful examination, in conjunction with the SSE location outcome log the SSE kiosk examiner will send the OIC an ‘Acquisition Feedback Form’ and a prepared ‘script’ which explains to the OIC the importance of completing the acquisition feedback form. ***Appendix B*** shows an example of a completed acquisition form; also user guidance and the template script which should be included in the body content of the email sent to OIC. It is advised that any email correspondence sent to the OIC is saved onto the sub-set folder of the CRIS folder generated, this provides an audit trail that the SSE kiosk sent an email to the OIC.

12.7 **OIC’s responsibilities around SSE Acquisition Form**
On completion of a successful examination, in conjunction with the SSE location outcome log, the SSE kiosk examiner will send via AWARE an email of the acquisition feedback form to the OIC.

Appendix B shows an example of a completed acquisition feedback form and provides guidance what tabs needs to be completed by the OIC. The ‘Send Response’ tab, if used, sends the completed form back to a generic email box called **‘Forensic Services - Kiosk Support’** - if done manually then the completed email can be used to send the completed feedback the OIC an ‘Acquisition Feedback Form’ in relation to the examination undertaken on the SSE kiosk.

12.8 **Completed acquisition forms**
Once the acquisition feedback from has been sent, the OIC is requested to review the output (report) produced by the SSE kiosk examiner and send back the completed acquisition form within 10 working days on receipt of the email. If after 10 working days the form has not been completed, a reminder will be sent to the OIC by DCC staff. If after a further 10 working days and no response is forthcoming from the OIC, then the escalation will be to the local SPOC and senior management team to deal with.

13. Statements

13.1 The SSE Kiosk examiner is responsible for completing a pro-forma statement for the exhibits examined, in order that the report/relevant content of the report can be used as evidence by the investigation Officer.

13.2 A template pro-forma statement can be accessed on the DCC shared drive on AWARE.

14. Useful contact details

14.2 DCC digital hub contacts (figure 4 refers) are available to provide technical support and advice regards to SSE kiosk examination procedures and the use of the SSE kiosk. The DCC digital hubs can be contacted Monday-Friday 8am-5pm - none urgent enquiries or feedback can be emailed to the dedicated mailbox ***Forensic Services - Kiosk support***

14.3 URGENT request for out of hours enquiries for assistance from DCC will be handled by MET Forensic Command (MFC) on Metropolitan 6

Digital Hub Location	Location covered	Contact Details	Digital Strategy Advisor	Contact Details
Croydon	South/South East	5		
Lewisham	South/South East			
Kingston	West/South West			
Wembley	West/South West			
Edmonton	East/North East			
Ilford	East/North East			
Charing Cross	Central			
Islington	Central			

(Fig 4. DCC Digital Hub contact information)

15. Legislation, Policy and Other Associated Documents

15.1 This guidance document provides a summary of our legal obligations set by the following legislation:

- Police and Criminal Evidence Act 1984 (PACE);
- Criminal Justice and Police Act 2001 (including the Supplementary
- Attorney General's Guidelines on Disclosure1)
- Criminal Procedure and Investigations Act 1996 (CPIA);
- Data Protection Act 1998 (DPA);
- Human Rights Act 1998 (HRA);
- Code of Practice on the Management of Police Information 2005, and the 2010 Guidance on the Management of Police Information (MOPI)

15.2 The processing is further underpinned by the following Codes of Practice, policy and guidance requirements:

- Forensic Science Regulator's Codes of Practice and Conduct for
- forensic science providers and practitioners in the Criminal Justice
- System2
- ACPO Good Practice Guide for Computer-Based Electronic Evidence 2012
- ACPO Authorised Professional Practice (APP) Information Management1
- http://www.attorneygeneral.gov.uk/Publications/Documents/Guidelines%20on%20di
- gitally%20stored%20material%20July%202011.doc.pdf
- 2http://www.homeoffice.gov.uk/publications/agencies-public-bodies/fsr/codes-practiceconduct?view=Binary
- NOT PROTECTIVELY MARKED
- ACPO (2005) Guidance on NIM, NIM Codes of Practice & NIM Minimum Standard
- ACPO guidelines for Digital evidence
- ACPO Data Protection Manual of Guidance
- MPS Guidance for Police Officers regarding the use of Territorial Police Mobile Phone Examination Facilities
- MPS Information Management Policy
- MPS Security Code Manual
- MPS Information Code of Conduct (and supporting FAQs)
- MPS Information Governance Framework
- MPS Information Policy Framework
- MPS Data Protection Compliance Standard Operating Procedures
- MPS Records Management Manual (including the MPS Review, Retention and Disposal Schedule)
- Management of MPS Intelligence Policy
- MPS Intelligence Strategy
- MPS Intelligence Manual
- ACESO guidance for Examiners
- Crimint via Metbats
- Local property disposal

16. List of Appendices

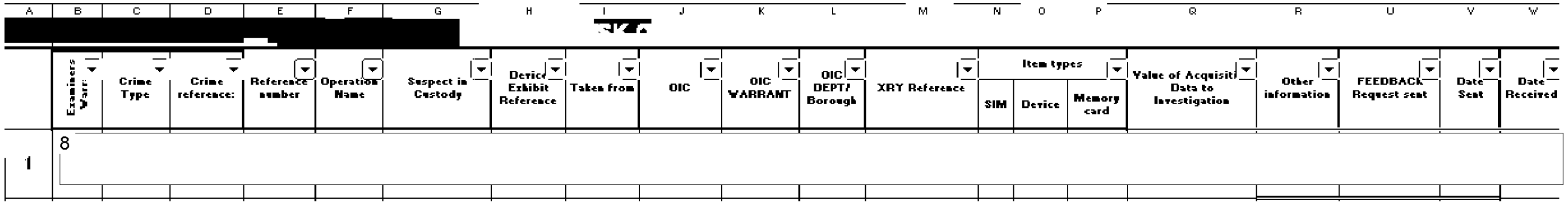
Appendix A - Summary of PACE POWER
Appendix B - Example of and SSE Kiosk Outcome Log
Appendix C - Example of an SSE kiosk Acquisition form

APPENDIX A; A SUMMARY OF PACE POWER

Section	Summary
Section 18(1)(a)(b)	Constables may enter and search premises occupied or controlled by a person under arrest for an indictable offence for evidence relating to that offence or some other indictable offence which is connected with or similar to that offence
Section 19(1)	These powers are exercisable by a constable lawfully on premises. A constable may seize anything on the premises he has reasonable grounds for believing has been obtained in consequence of the commission of an offence or is evidence relating to any offence AND it is necessary to prevent it being concealed, lost, tampered with or destroyed. However, Officers must note s19(6): No power of seizure conferred on a constable under any enactment (including an enactment contained in an Act passed after this Act) is to be taken to authorise the seizure of an item which the constable exercising the power has reasonable grounds for believing to be subject to legal privilege.
Section 22	Provides that anything seized for the purposes of a criminal investigation, including a mobile phone, may be retained for use as evidence at a trial for an offence or forensic examination or for investigation in connection with an offence.
Section 32(2)(a)	A constable shall have power to search an arrested person for anything which might be evidence relating to an offence
Section 32(2)(b)	If the offence for which he has been arrested is an indictable offence, a constable may enter and search any premises in which he was when arrested or immediately before he was arrested for evidence relating to the offence
Section 54	A custody officer shall ascertain, or cause to be ascertained everything a person has with him on arrival at a Police Station (under arrest or voluntary attendance). A custody officer may seize and retain items in the person's possession if the custody officer has reasonable grounds to believe that they may be evidence relating to an offence or believes that the person from whom they are seized may use them to cause injury, damage, escape, or interfere with evidence

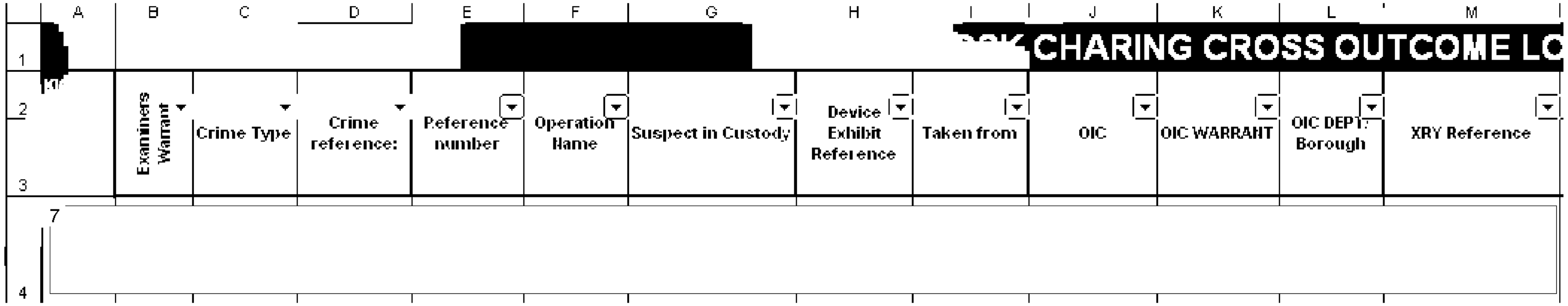
APPENDIX B: EXAMPLE OF AN SSE KIOSK OUTCOME LOG

Columns A - W



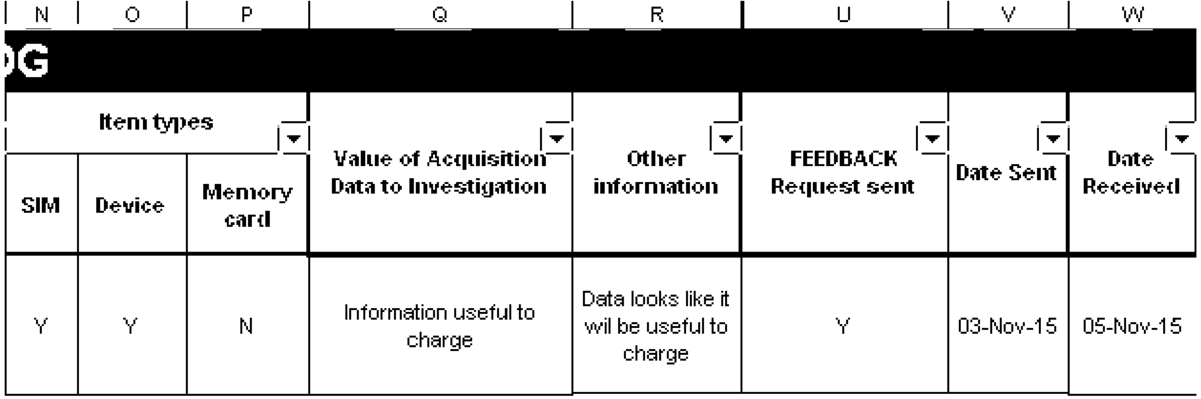
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	U	V	W
[redacted]																				
	Examiners Warr	Crime Type	Crime reference:	Reference number	Operation Name	Suspect in Custody	Device Exhibit Reference	Taken from	OIC	OIC WARRANT	OIC DEPT/ Borough	XRY Reference	Item types			Value of Acquisiti Data to Investigation	Other information	FEEDBACK Request sent	Date Sent	Date Received
													SIM	Device	Memory card					
1	8																			

Columns A - M



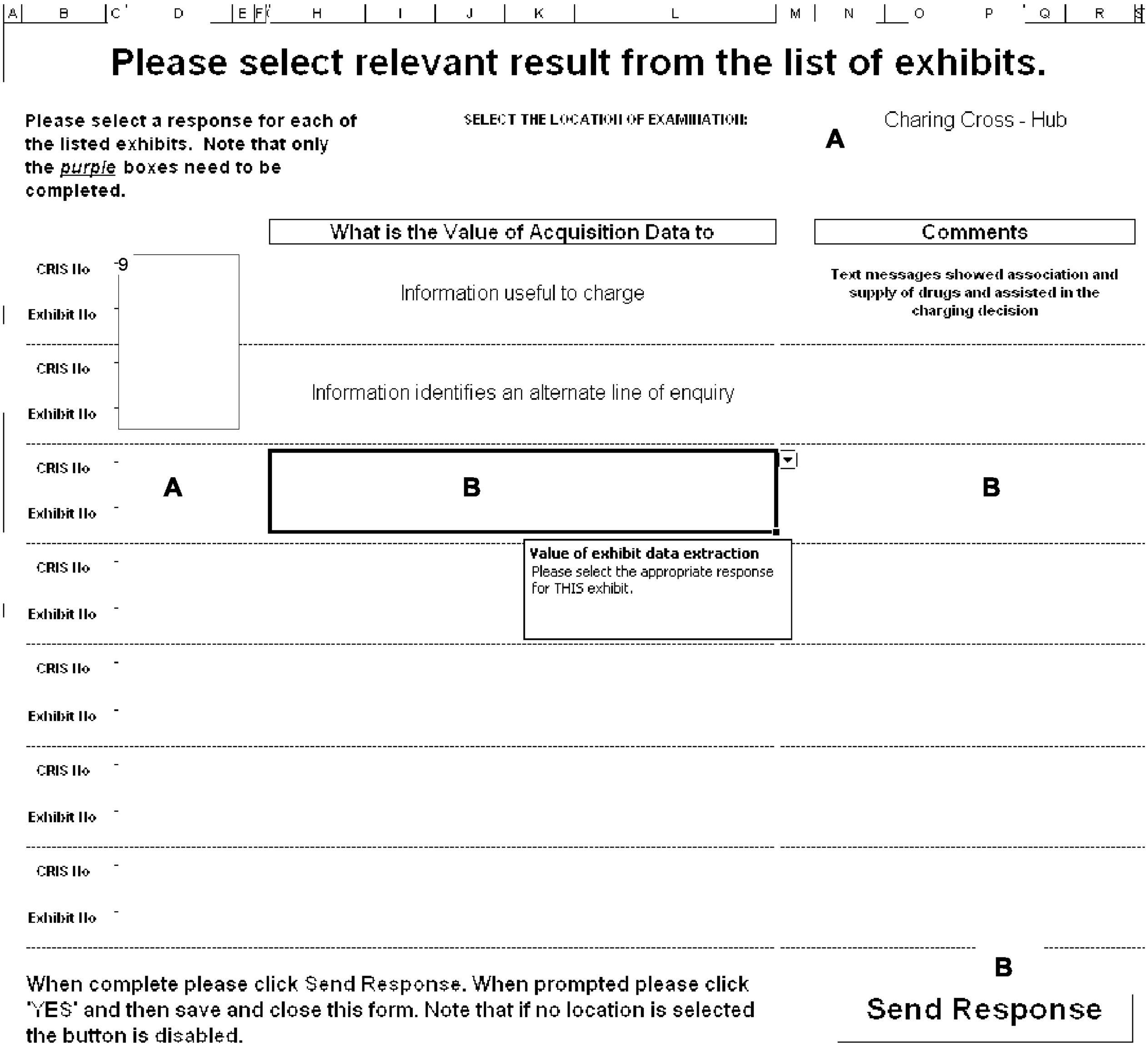
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	[redacted]				[redacted]					CHARING CROSS OUTCOME LO			
2 3		Examiners Warrant	Crime Type	Crime reference:	Reference number	Operation Name	Suspect in Custody	Device Exhibit Reference	Taken from	OIC	OIC WARRANT	OIC DEPT/ Borough	XRY Reference
4	7												

Columns N- W (Columns Q and W will be populated on receipt of the FEEDBACK request form if sent by DCC staff)



N	O	P	Q	R	U	V	W
OG							
Item types			Value of Acquisition Data to Investigation	Other information	FEEDBACK Request sent	Date Sent	Date Received
SIM	Device	Memory card					
Y	Y	N	Information useful to charge	Data looks like it wil be useful to charge	Y	03-Nov-15	05-Nov-15

APPENDIX C; EXAMPLE OF AN SSE ACQUISITON FEEDBACK FORM



Please select relevant result from the list of exhibits.

Please select a response for each of the listed exhibits. Note that only the *purple* boxes need to be completed.

SELECT THE LOCATION OF EXAMINATION: **A** Charing Cross - Hub

		What is the Value of Acquisition Data to	Comments
CRIS No Exhibit No		Information useful to charge	Text messages showed association and supply of drugs and assisted in the charging decision
CRIS No Exhibit No		Information identifies an alternate line of enquiry	
CRIS No Exhibit No	**A**	**B**	**B**
CRIS No Exhibit No			
CRIS No Exhibit No			
CRIS No Exhibit No			
CRIS No Exhibit No			

Value of exhibit data extraction
Please select the appropriate response for THIS exhibit.

When complete please click Send Response. When prompted please click 'YES' and then save and close this form. Note that if no location is selected the button is disabled.

B

Send Response

Guidelines for OIC Kiosk and SSE kiosk examiner

A = Indicates what needs to be completed by the SSE Kiosk examiner before sending the acquisition feedback form to the OIC:

- Select the location of Examination: Select the location where the examination took place (Drop Down)
- CRIS No: one entry for each exhibit examined
- Exhibit No: one entry for each exhibit examined

B = Indicates what needs to be completed by the OIC when received from the SSE kiosk examiner:

- What is the Value of Acquisition Data to: This is a drop down tab - select the appropriate response
- Comments: What specific in the report was of value and how it assisted, free text tab
- Send Response (Tab): The tab sends the intervention feedback form back to a generic email box 'Forensic Services - Kiosk Support', where the DCC staff will update the location outcome log where that examination was undertaken

APPENDIX C; EXAMPLE OF AN SSE ACQUISITON FEEDBACK FORM

Email Template sent with Acquisition Feedback Form

Dear (OIC Name),

Please find attached an 'Acquisition Feedback' form which relates to work recently conducted using the front line Kiosk support.

Feedback is important. It is essential as an organisation; we are able record accurate interventions in relation to the work undertaken, and also the value/relevance of the acquisition data to the investigation. Good news stories are generated from the feedback which is disseminated to SLT members at both a local and corporate level.

In order to navigate the form has been designed with 'simplicity' in mind; under the 'value of Acquisition Data to' tab, there is a drop down of each exhibit examined: (1) Information useful to Charge (2) Information useful to eliminate (3) Information identifies an alternate line of enquire (4) Information not useful in progressing the investigation - just hover over the one which applies and select.

The comments tab is 'free text' to allow specific feedback on the aspects of the report that impacted on the investigation e.g. text messages recovered identified associations with other associates and details of drug dealing taking place - this assisted in the charging decision but also provided new leads and the information was used in interview.

On the completion of the form please click the 'Send Response' tab and this will automatically send it to the hub mailbox - or the form can be sent directly back to the person who generated the feedback form. - PLEASE enable macros when requested.

It is appreciated that it takes time to read the acquired data; therefore feedback is requested within 10 days of the work being completed.

Your cooperation with this feedback form is appreciated, if you have any questions or queries regarding this form please contact the hub direct.

Kind Regards,

(Your Name)