Royal Mail Internal Information
Criminal Investigation Team

# 7.8 Recovering Computers, Mobile Phones & Digital Storage Devices for Evidential Purposes

Version 1.0 Final

27th January 2011

Review Date: 27th January 2013

Ray Pratt
Head of Investigations Policy & Standards
Royal Mail Security
Mobex
Mobile GRO

# Contents

## Key Accountabilities

| **Who is accountable?** | **What do I have to do?** | **When do I have to do this?** | **How do I do this?** |
|---|---|---|---|
| All members of Royal Mail Security | Ensure you comply with the procedures | Ongoing | As detailed within these procedures |

# Recovering Computers, Mobile Phones & Digital Storage Devices for Evidential Purposes

## 1. Introduction

**1.1** Vital evidence and intelligence can be obtained from computers, mobile phones and other digital storage devices. In order to maximise the value of such evidence and intelligence, Investigators must be aware of the correct procedures to be adopted when recovering such computers & devices. Following these procedures will ensure that any evidence obtained is admissible in Court.

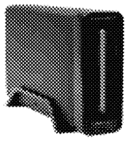
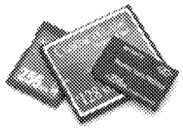
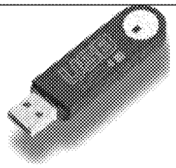
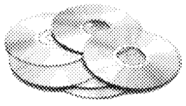
**1.2** The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Electronic Evidence outlines four principles when dealing with this type of evidence;

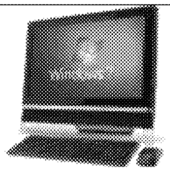
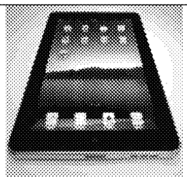
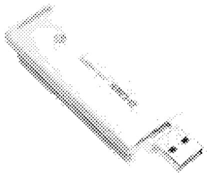
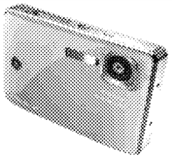
| | |
|---|---|
| **Principle 1** | No action taken by Investigators should change the data, held on a computer or electronic storage media, which may subsequently be relied upon as evidence in court. |
| **Principle 2** | Only competent persons should access any original data held on a computer or on electronic storage media and that person must be able to give evidence explaining the relevance and the implications of their actions. |
| **Principle 3** | An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. |
| **Principle 4** | The Investigator in the Case has overall responsibility for ensuring that the law and these principles are adhered to. |

**1.3** The Digital Forensics Team (DFT), Royal Mail Security have a full understanding of the obligations imposed in satisfying these 4 principles. The DFT is responsible for the examination and extraction of data from computers and digital storage devices. (Full contact details for the DFT are in section 5 below).

## 2. Digital Storage Devices

**2.1** There are many types of digital storage device that may be encountered whilst searches are being conducted. These not only include computers and mobile phones they also included such items as;

| | | | |
|---|---|---|---|
| **External Hard Drives**<br>(These give computers extra data storage capacity) |  | **Memory Cards**<br>(Available in many sizes) |  |
| **USB Sticks**<br>(Any item which has a USB connector is potentially a data storage device) |  | **CDs/DVDs** |  |

| | | | |
|---|---|---|---|
| **All in one computers** (This is where the digital storage device (hard drive) is contained within the monitor or screen) |  | **Electronic Entertainment Devices** (MP3 Players iPods and iPads Kindle digital book readers etc) |  |
| **3G Dongle** (Looks like a USB flash drive but contains a small slot where a SIM card fits) |  | **Digital Cameras** |  |

**2.2** The extent of search and seizure will be dependant on the type of offence being investigated and the evidence or intelligence available. Investigators are encouraged to consider what it is they are investigating, what evidence they are seeking and where that evidence is likely to be found. Investigators must ensure that their actions are justifiable and proportionate.

**2.3** If items are to be recovered from businesses advice, at an early stage, should be sought from the DFT.

## 3. Recovering Desktop and Laptop Computers

**3.1** **Initial action on recovering Desktop or Laptop PCs.** The initial action on discovering a PC which is to be recovered for evidential purposes is as follows;

**3.1.1** Ensure that suspects or other persons are unable to tamper with the PC.

**3.1.2** If printing allow the printing to finish.

**3.1.3** If it is deemed necessary photograph or video the scene or consider drawing a sketch plan.

**3.2** The subsequent action depends on whether the PC is **on** (see paragraph 3.3) or **off** (see paragraph 3.5).

**3.3** **Recovering Desktop and Laptops PCs which are switched off.** The following further actions should be carried out if the PC is switched off;

**3.3.1** Do **not** switch on the PC. (Make sure that the computer is switched off - some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on. If it is thought that the PC may be on then treat as in section 3.5 below).

**3.3.2** Be aware that some Laptops may power on by opening the lid, if the lid is closed do **not** open.

**3.3.3** Unplug the power and other devices from sockets on the computer itself (i.e. not the wall socket)

**3.4** Investigators should complete the process as described in paragraph 3.7 below.

**3.5** **Recovery of Desktop and Laptop PCs which are switched on.** The following process should be undertaken if the PC is switched on;

**3.5.1** If relevant, record what is on the screen by photograph or video, (if camera is available) and by making a written note.

**3.5.2** Do not touch the keyboard or click the mouse. If the screen is blank or a screen saver is present, the Investigator should decide if they wish to restore the screen. If so, a short movement of the mouse should restore the screen or reveal that the screen saver is password protected.

**a)** If the screen restores and it is relevant, photograph or video it, (if camera is available) and note its content.

**b)** If password protection is shown advice can be obtained from the owner/user as long the information is treated with caution. If the screen restores carry on as in **a)** above.

**3.5.3** Record the time and activity undertaken in respect of the screen.

**3.5.4** Shut down the computer by removing the power socket from the computer end.

**3.5.5** Note the time the computer was switched off.

**3.6** Investigators should then complete the process as described in paragraph 3.7 below.

**3.7 Completing the Recovery Process.**

**3.7.1** If the PC is a Laptop then the battery should be removed. (The power lead should be recovered).

**3.7.2** Recover all the items which may contain data such as external hard drives, USB sticks, DVDs etc. (If items containing data are attached to the computer by leads then recover the leads). There is no need to recover standard keyboards and the mouse unless required for forensic analysis (e.g. fingerprints).

**3.7.3** Search the area for diaries, notebooks or pieces of paper with passwords on them, which are often attached or close to the computer.

**3.7.4** Ensure that all items have signed completed exhibit labels attached to them to ensure continuity.

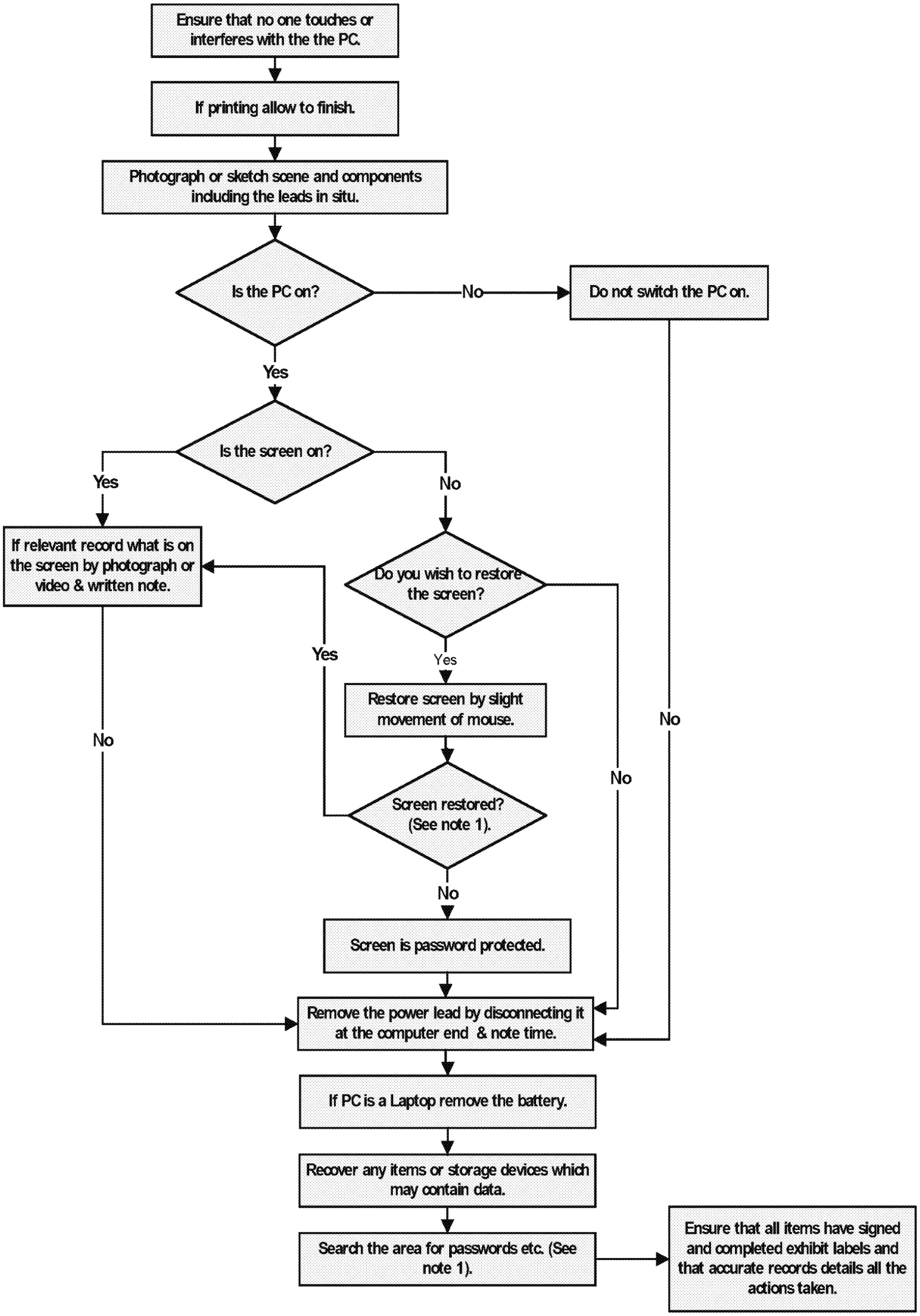
**3.7.5** **Ask the computer user for Passwords, PINs, User IDs and any encryption keys.** It is also advisable to recover operation manuals if these are available.

**3.7.6** Printers need only be recovered if required for forensic comparisons with printed documents.

**3.7.7** Investigators must ensure that they record accurately all the actions taken or information obtained in relation to the recovery of the computer equipment.

**3.8** Below is a process map which may be of use as an aide memoir. (Word copy associated for ease of reproduction).

## Process for Recovering Computers for Evidential Purposes


Ensure that no one touches or interferes with the the PC.
If printing allow to finish.
Photograph or sketch scene and components including the leads in situ.
Is the PC on?
No
Do not switch the PC on.
Yes
Is the screen on?
Yes
No
If relevant record what is on the screen by photograph or video & written note.
Do you wish to restore the screen?
Yes
Yes
Restore screen by slight movement of mouse.
No
No
Screen restored? (See note 1).
No
No
Screen is password protected.
Remove the power lead by disconnecting it at the computer end & note time.
If PC is a Laptop remove the battery.
Recover any items or storage devices which may contain data.
Search the area for passwords etc. (See note 1).
Ensure that all items have signed and completed exhibit labels and that accurate records details all the actions taken.

Process Map The
Recovery of Compute

## 4. Recovering Mobile Phones & Other Digital Storage Devices

**4.1 If Investigators are going to seize such devices they must not examine any data on the device themselves.** If they do they may be unnecessarily the changing data recorded on the device in breach of principle 1, (paragraph 1.2)

**4.2 Interception of Communications.** In addition to changing potential data Investigators should also be aware that there are Interception of Communication issues when examining devices used to access messages which are stored on electronic networks. These issues are understood by the DFT.

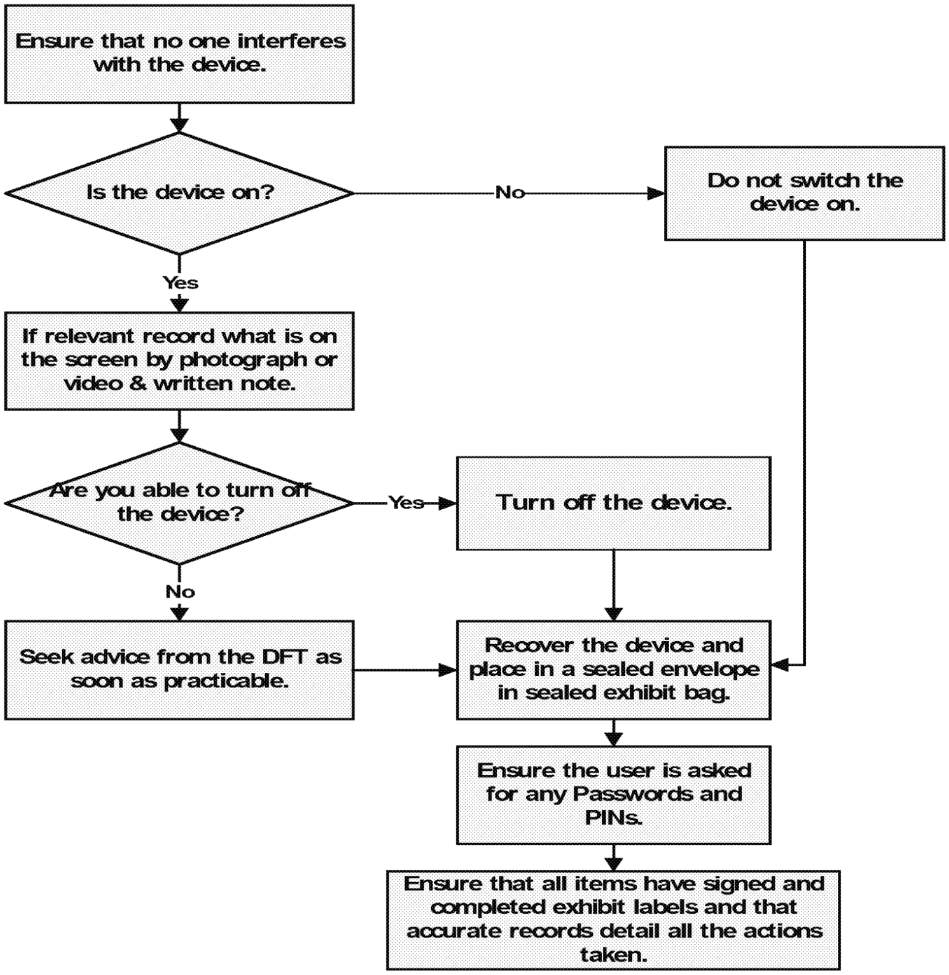
**4.3 Isolate from Mobile Network.** When recovering such devices the main point to consider is that they should be isolated from any "network" in order that the data on the device is not changed by receiving messages from the network (in accordance with Principle 1 at paragraph 1.2 above ). The best way to do this is to switch the device off. Of course, like with computers, if there is any data on the screen which is relevant then this should be recorded preferably by photograph or video, or if not by making a note. It is also important to note the time that the device was switched off and how it was switched off.

**4.4 Unable to switch off.** Some devices such as iPhones cannot be switched off and as such they cannot be isolated from the network. If this is the case then the time that the item was recovered must be noted. In these circumstances specialist advice from the DFT should be obtained as soon as practicable.

**4.5 If any devices are seized the Investigator must ask for any passwords or PIN access numbers.** Investigators should also recover power leads or other equipment such as "cradles" if they are needed to charge the device. Instruction books should also be recovered. Devices should be placed in a sealed envelope then placed in a sealed exhibit bag, which should be signed and completed to ensure continuity. Placing the device in a sealed envelope will help prevent it being switched on accidentally or deliberately by persons unauthorised to do so.

**4.6** Below is a process map which may be of use as an aide memoir. (Word copy associated for ease of reproduction)

## Process for Recovering Mobile Phones and Digital Storage Devices


Ensure that no one interferes with the device.
Is the device on?
No
Do not switch the device on.
Yes
If relevant record what is on the screen by photograph or video & written note.
Are you able to turn off the device?
Yes
Turn off the device.
No
Seek advice from the DFT as soon as practicable.
Recover the device and place in a sealed envelope in sealed exhibit bag.
Ensure the user is asked for any Passwords and PINs.
Ensure that all items have signed and completed exhibit labels and that accurate records detail all the actions taken.

Process Map The
Recovery of Mobile Pl

# 5. General

**5.1 Magnetic Field**s. Seized computers and digital storage devices should be handled with care at all times. Magnetic fields can interfere with data and as such contact with them should be avoided.

**5.2** Prior to the submission of a computer, mobile phone or digital storage device to the Digital Forensics Team the Investigator must complete a Digital Forensics Team Submission form GS308. Investigators should give details of the matter under investigation and the type of evidence or intelligence that they seek.

**5.3** Computers, mobile phones and other digital storage devices should be transferred to the Digital Forensics Team by hand. Contact details for the team are below;

| Address | Name | Telephone |
|---|---|---|
| **Digital Forensics Team**<br>**Royal Mail Security**<br>**Floor 2A Battersea SDO**<br>**202 Lavender Hill** | **Jo Dixon** | GRO |
| | | GRO |
| | **David R Brassington** | GRO |
| | | GRO |
| | **John Giddens** | GRO |

| | | |
|---|---|---|
| LONDON<br>SW11 1AA | | GRO |

POL00104896

# Change Control

| | |
|---|---|
| Status | Final |
| Version | 1.0 |
| Owner | Ray Pratt |
| Authors | Michael F Matthews |
| Release Date | 27th January 2011 |
| Document Privacy | Internal |

## Authorisation

| Title | Name | Signature | Date |
|---|---|---|---|
| Security | Ray Pratt | | January 2011 |

## Distribution List

| Name | Version | Date |
|---|---|---|
| All Royal Mail Security via Security Sharepoint | V1 | 27 Jan 2011 |
| | | |
| | | |
| | | |
| | | |
| | | |

## Documentation History

| | | | | | |
|---|---|---|---|---|---|
| *Issue* | V.1 | | | | |
| *Status* | Final | | | | |
| *Release Date* | 27/01/11 | | | | |
| *Effective From* | 27/01/11 | | | | |

## Document Change History

| Issue / Version | Summary of Change |
|---|---|
| V1 | Document Produced |
| | |
| | |
| | |
| | |

# Glossary

| Abbreviation or Term | Meaning |
|---|---|

| | |
|---|---|
| **DFT** | Digital Forensics Team |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## Document Summary

If you have any queries please contact:

Digital Forensics Team
Royal Mail Security
Floor 2A Battersea SDO
202 Lavender Hill
LONDON
SW11 1AA

Postline: GRO
STD: GRO
Fax: GRO