



## Good Practices for Seizing Electronic Devices

### *First Responder / Investigator*

#### *Mobile Telephones*

##### Identify Types of Devices

- Properly identify current types of mobile phones, batteries and accessories.

##### Preserve Evidence on Device

- Do not try to access the device.
- “ON/OFF RULE” What to do if device is on or off is a local or department issue.
- Record any information located on the screen of the device (write or photograph).
- Briefly ask subject for any PIN or personal code numbers.
- Look around the area for any PIN or related code numbers.
- Don’t let the subject touch the device for ANY reason.
- Properly label, store, handle and transport the device so no damage occurs.
- \*\*Take the evidence to the appropriate lab for examination as soon as possible, evidence could be lost when the battery dies.

##### Special Considerations Regarding this Device

- Are there any SMART/SIM cards at the scene.
- Look for batteries/power supply/cables/operators manuals/software and packaging.
- Does this item need to be tested for fingerprints or DNA? If so, use appropriate handling and evidence packaging procedures.
- Any questions regarding this electronic equipment at the scene, should be directed to a computer forensic examiner as soon as possible.
- Be aware of potential links between hand held computers and mobile phones.
- Any computer in the area may have synchronized information also contained on the device.

#### *Electronic Paging Devices*

##### Identify Types of Devices

- Properly identify current types of paging devices, batteries and accessories.

##### Preserve Evidence on Device

- Do not try to access the device
- “ON/OFF RULE” What to do if device is on or off is a local or department issue.
- Record any information located on the screen of the device (write or photograph).
- Don’t let the subject touch the device for ANY reason.
- Properly label, store, handle and transport the device so no damage occurs.
- \*\*Take the evidence to the appropriate lab for examination as soon as possible, evidence could be lost when the battery dies.

##### Special Considerations Regarding this Device

- Look for batteries/charger/operators manuals/software and packaging.

- Does this item need to be tested for fingerprints or DNA? If so, use appropriate handling and evidence packaging procedures.
- Any questions regarding this electronic equipment at the scene, should be directed to a computer forensic examiner as soon as possible.
- Identify the paging company as soon as possible to place a hold on the pager records.

### *PDA / Personal Digital Organizer / Handheld Computers*

#### Identify Types of Devices

- Properly identify current types of handheld computers, batteries and accessories.

#### Preserve Evidence on Device

- Do not try to access the device.
- “ON/OFF RULE” What to do if device is on or off is a local or department issue.
- Record any information located on the screen of the device (write or photograph).
- Briefly ask subject for any passwords, personal code numbers and type of operating system.
- Look around the area for any passwords or related code numbers.
- Don’t let the subject touch the device for ANY reason.
- Properly label, store, handle and transport the device so no damage occurs.
- \*\*Take the evidence to the appropriate lab for examination as soon as possible, evidence could be lost when the battery dies.

#### Special Considerations Regarding this Device

- Are there any associated devices (extended memory or expansion cards) at the scene.
- Look for batteries/docking station/power supply/cables/operators manual/software and packaging
- Does this item need to be tested for fingerprints or DNA? If so, use appropriate handling and evidence packaging procedures.
- Any computer in the area may have synchronized information also contained on the device.
- Be aware of potential links between hand held computers and mobile phone.
- Any questions regarding this electronic equipment at the scene should be directed to a computer forensic examiner as soon as possible.

### *Smart Cards*

#### Identify Types of Devices

- Properly identify current types of smart cards, accessories and readers/encoders.

#### Preserve Evidence on Device

- Do not try to access the device.
- \*\* If the smart card is connected to a reader/encoder or a computer contact a forensic examiner for advice.
- If connected to a computer, record any information located on the screen (write or photograph).
- Briefly ask subject for any passwords, personal code numbers.
- Look around the area for any passwords or related code numbers.
- Don’t let the subject touch the device for ANY reason.
- Properly label, store, handle and transport the device so no damage occurs.
- \*\*Take the evidence to the appropriate lab for examination as soon as possible.

### Special Considerations Regarding this Device

- Are there any associated devices (computers, readers/encoders) or other cards at the scene.
- Look for readers/encoders/power supply/cables/operators manual/software and packaging.
- Does this item need to be tested for fingerprints or DNA? If so, use appropriate handling and evidence packaging procedures.
- Any computer in the area may have synchronized information also contained on the device.
- Any questions regarding this electronic equipment at the scene should be directed to a computer forensic examiner as soon as possible.

## Forensic Examiner

### Mobile Telephone / PDA / Smart Card / Pager

#### Evidence Handling

- Follow normal handling procedures for forensic evidence.
- Check power/battery status on receipt.[where applicable]
- Be aware of other forensic procedures (fingerprinting, DNA).
- Be familiar with the device you are working on.
- Know your own limitations.
- Be aware that some devices may affect data on other items.

#### Examination Procedures

- Check with the first responder / investigator for passwords/PIN. [where applicable]
- Follow generic documentation procedures.
- Fully describe the device and other associated items.
- Examine the device with validated forensic tools and accepted forensic procedures.
- Use methods that minimize loss/change of data.
- Document findings.
- Perform quality review.

#### Training

- Training on forensic examination procedures.
- Training on examination equipment and tools.
- Training on the devices and their associated technologies.
- Training on presenting forensic evidence.
- Develop ongoing technical learning.
- Develop and maintain industry contacts.
- Perform competency and evaluation programs.

#### Proficiency Testing

- Participate in inter-laboratory proficiency testing programs.
- Conduct periodic quality audits.

#### Definitions

- Use internationally agreed terms and definitions.