

Guidelines in Cases of Suspected Mobile Phone Misuse



If the mobile phone is switched on

- Resist the urge to browse through the phone or try to preview evidence yourself.
- Turn the mobile phone off and do not turn it back on again.
- Make a note of the time you powered off the phone.

If the mobile phone is switched off

- Do not turn the mobile phone on.
- Do not remove the battery.
- Do not remove the SIM card.
- Do not remove the memory card.

Do not challenge the offender with your suspicions

- You may simply alert them and allow them to tamper with or destroy potential evidence.

Do not be tempted to let your own IT department have a quick look

- It is very tempting to ask for internal technical help to substantiate your suspicions before incurring any costs associated with seeking external help.
- Unless your IT department has the specialist forensic tools, experience and software, there is a very real risk that they could damage the evidence and render it useless in court or at a tribunal.

Treat it seriously

- Consider the individual under suspicion may have access to more than one device.
- Make a note of the time and date that you took possession of the phone.
- Place the phone in a sealed box and make one person custodian of the box.

Call in the experts

- CCL-Forensics can provide additional advice over the telephone or attend 24/7 in an emergency. The investigation can be open or covert depending on your circumstances. Complete discretion and confidentiality is assured.
- CCL-Forensics has a team of 36 experienced and fully trained Forensic Analysts, who provide services in both the private and public sector. Their accumulated knowledge and experience (more than 6,000 cases conducted) ensures that your evidence is in the safest of hands.

Guidelines in Cases of Suspected Computer Misuse



Treat it seriously

- Many offenders take the attitude that “it’s only a bit of fun”, however the risk to your business is not a laughing matter.

Keep it to yourself

- Unless anyone else internally really needs to know.

Do not challenge the offender with your suspicions

- You will simply alert them and allow them to tamper with or destroy potential evidence.

Do not be tempted to let your own IT department have a quick look

- It is very tempting to ask for internal technical help to substantiate your suspicions or before incurring any costs associated with seeking external help.
- Unless your IT department has the specialist forensic tools, experience and software, there is a very real risk that they could damage the evidence and render it useless in court or at a tribunal.

If the computer is switched off

- Do not turn the computer on. Every time a computer is switched on data will be changed. Computer forensic analysts use special forensic tools to ensure that when they investigate the computer, no changes are made to the digital evidence.

If the computer is switched on

- If there is anything visible on the screen, photograph it or make a note of it. Disconnect the power supply by pulling out the cable from the back of the computer.
- List all possible users of the computer and any other information you may have and make detailed notes of all actions taken in relation to the computer equipment. Consider asking if there are any passwords and record these carefully. Secure the items so they cannot be tampered with.
- Consider that the individual under suspicion may have access to more than one computer.

Call in the experts

- CCL-Forensics can provide additional advice over the telephone or attend 24/7 in an emergency. The investigation can be open or covert depending on your circumstances. Complete discretion and confidentiality are assured.
- CCL-Forensics has a team of 36 experienced and fully trained Forensic Analysts, who provide services in both the private and public sector. Their accumulated knowledge and experience (more than 6,000 cases conducted) ensures that your evidence is in the safest of hands.