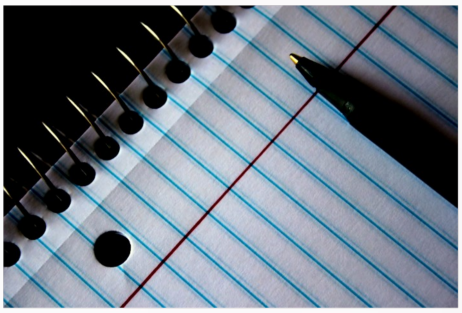

Computer Forensics Online Limited
Consulting Services
First Responders Guide to Employee Misconduct Investigations
For I.T & H.R Departmental Managers
Call today for a free, confidential consultation
(0800) 9996432 or (07517) 219269
enquiries@cf-online.co.uk www.iamconcerned.co.uk

# First Responders Guidelines

It is critical that digital evidential data is preserved during the early stages of an internal investigation. Following these guidelines will ensure that your investigation is not inadvertently compromised or contaminated by those first on the scene.

## STEP #1 - CREATE AND MAINTAIN A TIMELINE OF EVENTS



Before taking any action in relation to the investigation, create a detailed hand written timeline of events as they happen. Each person carrying out actions should produce their own hand written timeline.

This creates a critically important audit trail of your organisations actions, which can be used to demonstrate to opposing legal and forensic experts that evidential integrity has been preserved.

Key dates such as the date and time devices are seized must be recorded.

## STEP #2 - IMMEDIATELY SEIZE ALL EMPLOYEE DEVICES

Without delay immediately confiscate all company owned devices that the employee is using. These commonly include computers, laptops, mobile phones, tablets and USB storage devices. Also obtain any user passwords.

Do not allow an employee to continue using any device - even for a few minutes - this provides them with time to delete or modify evidence, leaving your organisation at a disadvantage should evidence be lost as a result. Notify them that any personal files will be returned at a later date.

Seized devices should be powered down and stored in a secure location.

## STEP #3 - DO NOT ACCESS THE SEIZED EMPLOYEE DEVICES


You are now in possession of a potential crime scene, depending on the type of misconduct your employee has carried out - fraud as an example.

Seized devices require specialist training and equipment in order to ensure they are duplicated and analysed in a forensically sound manner acceptable in a court of law.

Accessing the employee's devices by using your organisations I.T staff is a guaranteed way to destroy the integrity of any evidence you may find and will also contaminate the timeline stored on the seized devices as a result.

It is extremely common for an employee's legal representative to reject evidence that has not been collected by a qualified expert in a formal manner, on the grounds that it is tainted or has been tampered with.

It is our experience that evidence regularly becomes inadmissible, disputed or irreparably contaminated when it is not collected and analysed by a qualified digital forensics expert. Always call the experts.


Computer Forensics Online Limited

Consulting Services

Call Now

(0800) 9996432

Regent House, 2 Regent Road, Lowestoft, Suffolk, NR32 1PA - enquiries@cf-online.co.uk - www.iamconcerned.co.uk

# First Responders Guidelines

## STEP #4 - IMMEDIATELY CHANGE ALL EMPLOYEE CREDENTIALS


Prior to seizure of physical devices, coordinate both internally and with external vendors (such as a Data Centre) so that all passwords for any and all accounts the employee may have are changed at seizure time.

Login accounts to File Servers, Cloud Storage (such as Microsoft OneDrive), E-Mail, and Accounting Systems must all be changed. It is also critical to ensure that remote access is also revoked, such as VPN, Remote Desktop, LogMeIn and any other services that allow the employee to access company data from outside of the organisation (usually from home).

## STEP #5 - ENUMERATE EMPLOYEE OWNED DATA SOURCES


The employee must be asked to list all personal mobile telephones, laptops, tablets, E-Mail accounts and Cloud Storage accounts they own, which contain company data. Working with your legal team, ensure the employee is made aware that these items must be delivered "as is" to the company for expert inspection and sanitisation if necessary.

Company data stored on personal devices/accounts may constitute intellectual property theft, but in addition is a direct GDPR violation which can attract large fines - auditable sanitisation of these sources is critical.

## STEP #6 - CALL THE EXPERTS - COMPUTER FORENSICS ONLINE


Our computer forensic expert Mr Munsey has over 17 years experience of both Police and corporate investigations, you can rest assured that your case will be professionally, discretely and diligently investigated.

Mr Munsey will make forensically sound copies of any computers, mobile devices, online accounts (such as E-Mail or Cloud storage) and consolidate them to allow their contents to be searched and analysed for evidence.

Analysis usually takes between 3 and 14 days (depending on which service is chosen), before a report is produced detailing potentially relevant findings that can be used in a court of law, or an internal employment dispute hearing or tribunal.

**We offer all-in-one investigative packages, known as Device Activity Checks tailored to fit any dispute or case type, if you are investigating an employee - you need a DAC !**


Computer Forensics Online Limited

Consulting Services

Call Now

(0800) 9996432

Regent House, 2 Regent Road, Lowestoft, Suffolk, NR32 1PA - enquiries@cf-online.co.uk - www.iamconcerned.co.uk

# Which DAC Do You Need ?

There are three different types of DAC, Economy, Standard and Premium, with an Express service upgrade available at a significant uplift - deciding on which type you require is key to ensuring you get the most value and intelligence from your chosen DAC.

## ECONOMY

Economy is the entry level DAC, suited to simple cases such as those where the exact nature and timeframe of undesirable activity is already known by the client.

This package relies heavily on the client reviewing the user activity extracted from any given device. It is more suited to those with internal or outsourced I.T teams who wish to have their own findings verified and formally reported upon by an expert.

A rudimentary expert review of selected user activity and findings reported by E-Mail (no expert report) round off this package.

## STANDARD

Standard is the most popular DAC check, that focusses on detecting misconduct and intellectual property theft.

An in-depth review of all user activity extracted from the device submitted for examination is carried out.

A detailed expert report is produced, containing details of the most relevant activity and most notable unexpected findings.

Designed for non-technical clients who do not have any I.T resources to call upon, or wish to carry out a covert investigation and not involve their own staff.

## PREMIUM

Premium builds on the Standard DAC package and includes further expert review time.

In addition, all documents and E-Mails on the device are "indexed", which allows them to be keyword searched - imperative for cases where an employee's communication relating to a certain topic is sought.

Also included is a remote review facility, allowing clients to review relevant documents and E-Mails from the comfort of their own office. It is also possible for clients to download the material to view offline if required.


**Computer Forensics Online Limited**

**Consulting Services**

Call Now

**(0800) 9996432**

Regent House, 2 Regent Road, Lowestoft, Suffolk, NR32 1PA - enquiries@cf-online.co.uk - www.iamconcerned.co.uk

# Expert Credentials

## Jon Munsey
## Digital Forensics Expert

I have over seventeen years experience as a computer forensics crime investigator.

My background as a senior ex-Police computer forensics expert means I have successfully investigated hundreds of both corporate and criminal matters over the years.

I am now a specialised intellectual property and employee misconduct investigator. I also frequently investigate other matters such as corporate espionage, serious fraud, cyber-crime and hacking. My court experience is broad, I have acted as an expert on cases heard in Magistrates, Crown, High and the Supreme courts.

Over ten years ago I started my own consulting company **Computer Forensics Online (CFO)** to provide a bespoke, highly personalised and discreet service to clients worldwide.

I have built a strong reputation for delivering a quality, yet cost effective service to my clients - which includes heads of state, government agencies, business executives, celebrities and other high net worth individuals.

**Computer Forensics Online Limited**

**Consulting Services**

Call Now

(0800) 9996432

Regent House, 2 Regent Road, Lowestoft, Suffolk, NR32 1PA - enquiries@cf-online.co.uk - www.iamconcerned.co.uk