BDG Investigator's Bulletin

EDITION 3 · JUNE 2026

Welcome to the June 2026 edition of the BDG Investigator's Bulletin. In this edition we explore three core themes from our Investigation Essentials Training programme. We begin with the Golden Hour — the critical window immediately after a report is received, when the right actions can make or break an investigation. We then examine the building blocks of a sound investigation, including the five immediate priorities every investigator must address at the outset of any case. Finally, we turn to digital disclosure — covering the leading Court of Appeal authorities of R v Richards [2015] and R v Bater-James [2020], the key principles they establish, and the framework set out in Annex A of the Attorney General's Guidelines on Disclosure (updated February 2024). As always, we hope this edition supports your CPD and your day-to-day practice.

The Golden Hour

CORE INVESTIGATIVE PRACTICE

The Golden Hour describes the critical window immediately after an incident or report is received — when the right actions, taken promptly, can make or break an investigation. The term originates from emergency medicine but has long been embedded in investigative practice.

For local and public authority investigators — trading standards, housing, environmental health, licensing, counter-fraud etc — the same principle applies. Evidence can disappear quickly. Scenes change and witnesses' memories fade. The Golden Hour mindset focus investigators to act with purpose from the moment a report lands. Some considerations are:

Victims, Witnesses & Suspects

Identify, risk-assess, safeguard.

Take initial account 5WH, secure evidence.

Scene preservation

Identify, preserve and secure evidence.

Photograph, video, maintain log.

Securing evidence

Physical, documentary and digital evidence.

Preserve integrity of digital evidence.

Records

Record all decisions with rationale

Pursue fast track actions.

Intelligence

Inform risk and threat assessment.

Use open source and local intelligence checks

A key question that often goes unasked: what do you record when you decide NOT to do something? These are often the decisions that get challenged in court and how your record this can protect your investigation.

Building Blocks of a Sound Investigation

CORE INVESTIGATIVE PRACTICE

Every investigation is unique, but the foundations are consistent. Investigation essential principles provide a framework that applies to any investigator, in any organisation. At its core is one principle:

> **Assume nothing | Believe nothing | Challenge everything**

The key building blocks include:

Professional curiosity

The discipline of asking 'why?' and 'what else might explain this?'

The 5WH framework

Structuring your investigation around Who, What, Where, When, Why and How

Hypothesis building

Developing and testing more than one explanation for what happened

Gap analysis

Knowing what you know, what you don't know, and what that means for your lines of enquiry

Record keeping

Comprehensive, contemporaneous and objective documentation of every decision

The Five Building Blocks of Initial Investigations

CORE INVESTIGATIVE PRACTICE

Alongside the investigative building blocks, every investigator must consider five immediate priorities at the outset of any investigation. These apply regardless of the type or scale of the case — from a trading standards complaint to a complex counter-fraud investigation.

Preserve Life

The safety and welfare of any person at risk must be the immediate first priority. Consider whether anyone requires urgent medical attention, safeguarding intervention or protection from ongoing harm.

Preserve Scenes

Identify and secure any scene relevant to the investigation without delay. A scene that is not preserved promptly may be contaminated, altered or lost — taking with it evidence that cannot be recovered.

Secure Evidence

Physical, documentary and digital evidence must be identified and secured at the earliest opportunity. Consider what exists, where it is held and what steps are needed to prevent loss, destruction or tampering.

Victims and Witnesses

Identify all victims and witnesses promptly and consider their immediate needs, including safeguarding and vulnerability. Take initial accounts as soon as practicable — memories fade and accounts can be influenced over time.

Suspects

Identify the suspect or subject accurately and completely — full name, role, address, associates and any relevant intelligence. Consider whether early action is needed to prevent ongoing harm, evidence loss or interference with witnesses.

CORE INVESTIGATIVE PRACTICE

Fast Track Actions

Fast track actions are those which, if not pursued immediately, will result in the loss of evidence or the opportunity to progress the investigation. The following areas should be considered at the outset of any local authority or public sector investigation.

Victim / Complainant

Immediately assess safeguarding needs and identify any ongoing harm. Take a brief initial account using the 5WH framework and secure any evidence the complainant already holds — receipts, messages, photographs or contracts. Consider whether other victims may exist.

Location / Scene

Attend and secure the premises without delay — subjects may move on and records can disappear quickly. Record the scene as found using photographs, video and notes. Identify and preserve time-sensitive sources such as CCTV, access logs and till data before they are lost or overwritten.

Suspect / Subject

Verify the subject's full identity including any trading name, professional role, addresses, vehicles and associates. Check for prior intelligence and enforcement history. Preserve the digital footprint — websites, social media and online listings — and record every decision made, including decisions not to act immediately.

R v Richards & Others [2015] EWCA Crim 1941

LEADING COURT OF APPEAL AUTHORITY

The Case

A large-scale fraud investigation resulted in the seizure of numerous computers. Despite the prosecution case being served, the matter did not progress beyond primary disclosure for five years. The sheer volume of digital material — 7 terabytes — was never properly managed. The trial judge stayed the prosecution as an abuse of process.

The Significance

The Court of Appeal used this case to issue definitive guidance on how the criminal justice system must handle digital disclosure obligations under the CPIA. It remains the leading authority on managing voluminous digital material in complex criminal prosecutions.

> **Disclosure is not an end-of-investigation task. It must be planned from day one.**

Key Principles for Investigators

INVESTIGATION LAW · CASE NOTE

The lessons from Richards apply to any investigation involving digital material — regardless of scale. The obligations under the Criminal Procedure and Investigations Act 1996 (CPIA) do not diminish because a case is smaller. These are the five principles every investigator must apply:

Identify early

Identify digital material at the start of every investigation, not at pre-charge stage

Preserve properly

Seize and preserve digital evidence in a forensically sound way, with a clear chain of custody

Review proportionately

You do not need to examine everything, but you must record your approach

Engage early

Engage with the prosecuting authority early in any case involving significant digital material

Unused material counts

Unused digital material still triggers disclosure obligations — material that undermines the prosecution or assists the defence must be revealed

The principles established in R v Richards & Others [2015] EWCA Crim 1941 remain the foundation for managing digital disclosure in complex investigations. R v Bater-James [2020] EWCA Crim 790 builds on and reinforces those principles. Annex A of the Attorney General's Guidelines on Disclosure (updated February 2024) sets out the definitive framework for investigators and prosecutors handling digital material. These obligations apply to all local authority and public sector investigators. These topics are covered in detail in BDG's Investigation Essentials Training.

R v Bater-James & Anor [2020] EWCA Crim 790

DIGITAL DISCLOSURE · CASE NOTE

Case: R v Bater-James & Anor [2020] EWCA Crim 790 — Court of Appeal (Criminal Division)

Issue: The Court of Appeal issued authoritative guidance on the duties of investigators and prosecutors in managing digital material, building directly on the foundations laid in R v Richards [2015].

Bater-James is now the leading modern authority on digital disclosure obligations. The Court set out a clear framework for how investigators must approach digital material — from the moment it is identified through to unused material review. For local and public sector investigators, the principles are directly applicable regardless of the scale of the case.

The Four Key Principles

Principle One — Reasonable Lines of Enquiry Only

Digital material should only be reviewed in pursuit of a reasonable line of inquiry. There is no presumption that a complainant or witness's device should be inspected — there must be a properly identifiable foundation, not mere conjecture or speculation. Material should only be disclosed if it meets the disclosure test.

Principle Two — Staged and Proportionate Approach

Investigators should adopt a staged and proportionate approach. Wholly irrelevant material should not be reviewed. Consider whether the digital material can be reviewed without taking possession of the device. Where a device is necessary, contents should be downloaded with minimum inconvenience and returned without unnecessary delay.

Principle Three — Keep the Witness Informed

The witness or complainant should be kept informed throughout. They should be told how long the device will be retained, what will be extracted, what will be examined and what may be disclosed. Material will only be provided to the defence if it meets the test for disclosure and has been suitably redacted.

Principle Four — Consider the Consequences of Refusal

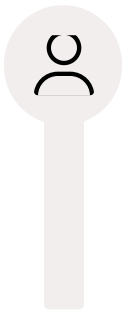
If a witness refuses to provide access to their device, investigators should explain the procedure and consider whether a witness summons is appropriate. Where material is not provided or is deleted, the court may consider whether proceedings should be stayed on the basis that a fair trial is impossible.

Annex A of the Attorney General's Guidelines on Disclosure (updated February 2024) provides the definitive framework for managing digital material. It sets out the obligations on investigators and prosecutors from the point of seizure through to trial. It is essential reading for any investigator handling digital evidence. Access the Attorney General's Guidelines at: www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure

Digital Disclosure — Key Actions for Investigators

DIGITAL DISCLOSURE · PRACTICAL GUIDANCE

Digital disclosure is a time-consuming and complex exercise. Unless it is addressed from the earliest stage of an investigation, it may not be possible for a prosecutor to be satisfied that the disclosure exercise can be completed properly before trial. The following key actions should be considered from the outset.



Start Early

Investigators should consider disclosure from the earliest opportunity. Unless the digital disclosure process is at a well-advanced stage prior to a charging decision, there may be insufficient time between charge and trial for the exercise to be properly completed.

Complete an Investigation Management Document (IMD)

In cases involving large amounts of digital material, investigators are encouraged to complete an IMD to outline the approach being taken to reasonable lines of enquiry. This sets out the digital strategy and ensures transparency of approach.

Handle Digital Material Correctly

No action should be taken which changes data on a device that may subsequently be relied upon in court. An audit trail must be kept of all processes followed. If original data must be accessed, it should only be done by someone competent to do so and able to explain their actions to a court.

Use a Proportionate Review Strategy

Investigators are not required to examine all digital material. It is proper to search by sample, key words or other analytical techniques to locate relevant material. Search terms must be carefully selected — not too generic — and the approach must be documented and defensible.

Escalate Resource Concerns Early

Digital disclosure may require additional resources and specialist software. Any concerns about the level of resources being applied to the disclosure exercise should be escalated without delay. Early advice from the prosecutor is strongly recommended in cases involving extensive digital data.

Digital Disclosure — Seizure, Documentation & Record Keeping

DIGITAL DISCLOSURE · PRACTICAL GUIDANCE

Proper seizure, handling and documentation of digital material is essential to the integrity of any investigation. The following principles — drawn from PACE 1984, Annex A of the Attorney General's Guidelines and the case law — set out what investigators must do.

Seizure and Imaging

Where possible, a forensically sound image of digital material should be taken at the location of the search. The seizure of computers may have a detrimental effect on a business's ability to operate , care must be exercised. Where an image is taken on site, the original need not be seized. Where originals are taken, investigators should copy or image the material for the owners when reasonably practicable under PACE 1984 Code B 7.17 (*where PACE powers are exercised"* or *"or equivalent provision under the relevant statutory power)*

Record Everything

A record or log of all digital material seized or imaged must be kept and shared with the prosecutor. In cases involving large volumes of data, the digital strategy — including sampling techniques, key word searches, software used and the reasons for search categories — must be set out in an IMD and subsequently a Disclosure Management Document (DMD).

Search Terms and Sampling

Where large volumes of material exist, it is proper to search by key words, sample or other analytical techniques. Search terms must be targeted and not too generic. Where dip sampling is used, it must be statistically robust and capable of repetition. The defence should be invited to agree search parameters and identify potential search terms.

Transparency and Early Dialogue

The prosecution should encourage early dialogue with the defence about what has been considered reasonable in the circumstances of the case. The approach taken must be made explicit in a Disclosure Management Document. It is never appropriate to simply supply images of devices to the defence to conduct their own disclosure exercise.

Investigation Essentials Training

BDG TRAINING CONSULTANCY

These topics and much more, are covered in BDG's Investigation Modular Essentials Training programme, designed specifically for local, public and private investigators. Practical, plain English, and built around the challenges you actually face. Please see our range of Investigation Essentials Training courses and workshops at www.bdgtrainingconsultancy.co.uk

To find out more or book a free training consultation for your team, please email info@bdgtrainingconsultancy.co.uk

BDG Training Consultancy Limited

Overt & Covert Investigation | Training & Development

Email: **info@bdgtrainingconsultancy.co.uk**

Website: **www.bdgtrainingconsultancy.co.uk**

Registered in England and Wales

Company Number: 10475761

VAT Registration: GB 430302261