The Golden Hour

This is a term for the period immediately following the commission of an incident or an offence when material is abundant and readily available.

Positive action in the period immediately following the report of a crime or breach of company policy minimises the attrition of material and maximises the chance of securing material that will be admissible in court, discipline or internal procedures.

All material may be judged to be admissible under certain circumstances.

There are a number of general principles, however, which mean that some material may not pass the evidential test for example hearsay testimony, intelligence reports or evidence of opinion.

Even though the material is of a type that is generally not admissible, it does not mean that it should not be gathered or that it will not assist the investigation. Such material may be highly valuable in setting parameters for other investigative activities or generating lines of enquiry that may produce other relevant, reliable and admissible material, and should, therefore, always be gathered.

Fast track actions
During the golden hour period there are a number of actions which, where possible, require an immediate response by the person initially contacted (the Responsible Person) or the Investigating Officer.

If you are investigating a health and safety incident, bullying, harassment, corruption, assault, damage to property etc. there is usually a scene or multiple scenes where the event took place.

Although every case differs the following actions are recommended:

· Visit and preserve the scene to restrict access and enable the gathering of forensic evidence it may become part of an external agency investigation.

· Draw a sketch plan of the scene.

· Take photographs or video the scene.

· Ensure the seizure and securing of documents, computer and telecoms data.

· Establish who had access at the time.

· Secure any incident reports, duty rosters or CCTV

To ensure and maintain the integrity of the investigation actions the following should be considered:

· Restricting staff members access to IT systems.

· Restricting staff members access to buildings/ offices.

· Relocate staff members.

· Suspension of staff members.