Workplace Investigations

A guide from Insight HR

www.insighthr.ie

InsightHR

Contents

Workplace Investigations - A Guide

A workplace investigation is a fact-finding exercise which can be fraught with difficulty. They can take many forms and may take place for many reasons.

It is important when confronted with an issue or a complaint that the employer quickly assesses the situation and decides whether a formal investigation is necessary or not. Not every complaint or incident requires a formal investigation. It is, however, important to be aware that there are risks in incorrectly deciding not to investigate a matter.

A formal workplace investigation may be necessary when:

- An employee complains of bullying, harassment or sexual harassment at work and the issue(s) cannot be resolved informally or through mediation.
- You suspect an employee is stealing from the business or is engaged in some form of fraudulent activity in the workplace.
- There are serious issues of misconduct which could lead to the dismissal of one or more employees.

Many companies rely on their internal HR departments or senior managers to conduct workplace investigations. This can be a sensible and economical approach to take – provided of course that the managers conducting the investigations are properly trained, are capable of taking an objective and impartial approach to the investigation and are not involved in the suspension, discipline or dismissal of that employee at a later date.

"Running a workplace investigation is complicated and can be intimidating. We completely understand this.

With over 20 years of experience in running both onsite and virtual workplace investigations, we know that the more sensitive the issue the higher the risk. We also know all the problems that running an inadequate investigation can cause, and we can help you to navigate this dangerous territory."

Mary Cullen - Managing Director of Insight HR

The cost of getting it wrong

The Labour Relations Commission's Code of Practice on Grievance and Disciplinary Procedures recommends that employers have a procedure for dealing with grievances and disciplinary issues and provides significant guidance to employers on the appropriate components of such procedures.

Though not legally binding, the provisions of the Code of Practice are being used by the bodies such as the WRC and High Court in adjudicating on cases relating to disciplinary issues, for example, claims of unfair dismissal. The bar has been set such that employers need to be able to demonstrate that they have complied with the provisions of the Code of Practice.

But what happens if an employer fails to follow the procedure properly? Or if the employer's procedure is deemed to have been flawed in some way? Either of these can result in the employer failing to defend themselves successfully against a claim of unfair or constructive dismissal. The financial impact of such rulings can be severe – potentially far outweighing the cost of ensuring that a proper procedure is in place and is followed correctly. And, of course, there can also be significant reputational damage when rulings enter the public domain.

There is ample precedence in case law to show that employers can lose a case even if they have a strong or compelling argument. The strength of any case they have against an employee is downplayed and can even be deemed irrelevant if their actual procedure is deemed flawed.

A recent example of this is the case of a technical services manager whose claim for unfair dismissal eventually made its way to the Labour Court, where he was awarded €25,000, even though there was evidence that he had breached his contract of employment and lost the trust of his employer by overstating his hours of work and falsifying company records.

When the business became aware of this evidence, the matter was investigated, during which time the employee was suspended from work. Following this, there was a disciplinary meeting which resulted in the employee's subsequent dismissal. However, the Labour Court found that correct procedure had not been followed, namely that:

- The employee had not been given sufficient notice of the investigatory meeting during which he was notified of his suspension.
- He was not advised to bring a representative, nor was he advised of the potential implications of the meeting.
- The organisation allowed one particular management representative to take part in both the investigatory and disciplinary meetings.

The employee had suffered significant financial losses as the result of his dismissal, which were outlined to the Court, these amounted to almost €99,000. However, as the Court found that the employee had contributed to his own dismissal, the award was

reduced to €25,000. Despite this, €25,000 is still a significant award which could have been avoided.

In another example, a store manager was awarded €6,500 for unfair dismissal after being sacked for gross misconduct. In this case, his employer, a restaurant chain, had received a complaint from an employee that the store manager had been sexually harassing her, turning up at her house uninvited and threatening to cut her hours of work.

Upon investigation, it emerged that the store manager had used his seniority in the business to extort sexual favours from his staff. He even admitted to this in his investigation interview. After the investigation, the restaurant chain dismissed the store manager, in line with the company policy on gross misconduct.

The WRC found that, although the store manager's misconduct was serious enough to warrant his dismissal, the failure of the restaurant chain to follow fair procedure meant that ultimately the process was flawed. The Adjudication Officer cited the following issues:

- The restaurant chain had not provided the store manager with full details of the allegations against him, nor the seriousness of the matter and its potential outcome.
- The investigation meeting was not escalated to a disciplinary meeting.
- The store manager was not informed of his right to representation nor to defend himself.
- The store manager was not provided with the name of the person to whom he should address an appeal.
- The store manager was not given the opportunity to cross-examine the witnesses.

Both these awards could have been avoided if the companies had followed fair procedures. The route to mitigating risks of these sorts of judgements occurring to an employer is obvious:

1. Employers should be familiar with the Code of Practice.

2. Employers should have their own grievance and disciplinary procedures defined and written down.

3. The procedure should comply with the Code of Practice and should be fair and reasonable. For example, even if the procedure fairly and reasonably defines elements that comply with the Code, the procedure needs to reach the same level of fairness and reasonableness for any elements above and beyond what is mentioned in the Code.

4. Employers need to be able to demonstrate that the procedure is used in the case of grievance and disciplinary proceedings.

"Do I need to involve the Gardai?"

Take the unfortunate case in Donegal, where a woman was imprisoned for two years after stealing the sum of €760,000 from her employer over a six-year period. It wasn't until several years after the first incident of theft, when a new director at the company noticed large sums going missing, that the matter was investigated. In this case, the woman was working as an accounts administrator and had access to multiple bank accounts. Even so, it's still a significant sum to go missing without being noticed, and just goes to prove how difficult it can be to detect workplace theft.

While this is an extreme example, theft in the workplace can actually come in many different forms including taking stock without paying for it, not documenting sales properly, stealing customer details such as credit card numbers, and much more.

Theft can even present itself as seemingly innocuous actions, such as abusing the sick leave policy by taking paid time off for illness when not really sick, timewasting while working by carrying out another job during working hours and making excessive personal phone calls from a company phone.

With so many definitions of workplace theft, how do you know which instances warrant legal action?

Proceed with caution!

First and foremost, remember to proceed with caution. There could be a reasonable explanation, and the last thing you will want is to have a case of unfair dismissal on your hands. Even if you have undeniable evidence that an employee has stolen from the business, there are still proper procedures that must be followed before any disciplinary action is taken. The employee has a right to a fair and impartial investigation and to review and respond to any evidence against them.

If an investigation is conducted and it is found that an act of theft has occurred, and the employee is subsequently dismissed, then they have a right to appeal the decision.

Those working in the HR function will no doubt appreciate the importance of having relevant policies and procedures in place, such as a Discipline Policy and an Honesty Policy. These must be documented and communicated to employees when they first begin work.

An employee suspected of theft should also be reminded of the relevant procedures.

Reporting to the Gardai

Where the potential risk to the business is low, the most reasonable course of action for a business to take may be to launch an internal workplace investigation first in order to determine whether wrongdoing has actually occurred. There are a few reasons for this. From a business perspective, you may want to consider the effect that it will have on the workforce if you involve the guards without ascertaining the full facts of the matter –

especially if it is discovered that the allegation is unfounded. Another reason is that the guards are also dealing with civilian crime, and it's possible that an allegation of theft in the workplace may not be first on their list of priorities. Remember too that when a criminal investigation is launched, the employee will likely seek legal representation. That representative may advise the employee to only discuss the matter with the Gardai or to simply refuse to comment during a workplace investigation. That means that any internal investigation into the incident may be delayed. The civil law standard for proof is the balance of probabilities, while in criminal law the standard is beyond a reasonable doubt. If there is not enough evidence to convict an employee in a criminal law setting, it may add complexity to the workplace investigation.

With all that said, if a serious crime is suspected, or there is a danger that evidence may be destroyed, falsified, concealed or disposed of, it is advisable to report it to An Garda Síochána immediately. Leaving it too late to report can mean that it is significantly more difficult to prove that any theft has occurred. As the criminal law standard requires proof beyond a reasonable doubt, any tampering of evidence can have serious consequences to the investigation of the case. Of course, the decision on when to involve the gardai should be made on a case-by-case basis depending on potential risk to your business and the likelihood of wrongdoing occurring again while the matter is investigated.

If you suspect an employee of theft, then you have a right to report it to the gardai. Moreover, it is actually mandatory under the Criminal Justice Act 2011 s.19 for all companies to report information they know or believe might be of material assistance in preventing the commission by a person of a 'relevant offence' e.g., theft or fraud, or securing the apprehension, prosecution or conviction of a person. The maximum penalty for an offence is an unlimited fine and imprisonment for up to 5 years or both. Employers should not ignore their reporting obligations and should seek advice at the earliest opportunity.

Important points to consider

An act of gross misconduct is one which breaches the trust between an employer and their employee(s). That means that if a breach of trust is proven to have occurred, then it doesn't matter whether it was a post-it note someone stole or a large sum of money.

Consider the supermarket employee who lost his job for stealing some sweets from a tin of Celebrations. He brought a case of unfair dismissal against his employer; however the WRC dismissed the action, having found that the man had received proper prior warning that the company had a zero tolerance for theft.

In a similar incident, a hotel worker was discovered to have taken two cups of coffee powder from the hotel kitchen. As the hotel had a zero-tolerance policy he was dismissed for gross misconduct, and a later appeal to the EAT (now known as the WRC) was unsuccessful.

In both of these cases, the item that was stolen may be considered to be inconsequential to the business. However, any business with robust policies and procedures that make it clear that any theft is considered an act of gross misconduct – and this fact has been communicated to employees and proper procedure followed – will likely find themselves in a much better position to defend any later claims of unfair dismissal.

Investigating bullying complaints

Obviously, prevention is better than cure. However, no matter how many preventative steps HR can proactively take, it will never be possible to completely eradicate all possibility of bullying. The important thing is that there is an open culture of respect, and that employees always know what action they can take to help resolve matters.

Should a complaint be received, the organisation has an obligation to follow procedure as outlined and communicated to staff through an anti-bullying policy. Both an informal and formal procedure should be defined by the employer and captured within the policy. If the company has not defined these processes, it will be unable to deal adequately with the complaint.

It is the employee's choice as to which of the two processes to use. As the name suggests, the goal of the informal process is to resolve the situation as informally as possible. If this succeeds, it minimises the conflict and stress involved. As suggested in the new Code of Practice on the Prevention and resolution of Bullying at Work, organisations with adequate resources can appoint a support contact who can act as an unbiased advisor to employees who wish to discuss their options before taking the matter to HR. This can be an invaluable tool in helping employees feel comfortable about seeking a resolution, and can also help them to identify whether to choose an informal or formal process.

The informal process normally involves the employee dealing directly with the alleged perpetrator with the aim of resolving the situation promptly and in a low-key fashion. However, someone who is being bullied may find it difficult to approach the perpetrator. Mediation could be an option, as could informal meetings facilitated by management. It is important to remember to keep a strong paper trail, even if the process is informal, as it may help to show that there was an attempt to resolve matters. If the employee is unhappy with the outcome of the informal process, or bullying continues, or if the employee wishes to bypass the informal process entirely, then the formal process is followed. With the formal process the complainant makes the complaint in writing. The complaint should be made to their immediate manager or supervisor or to someone else in a management role, if, for example, that supervisor is the alleged perpetrator. At this stage, the company should not draw any conclusions. Both parties deserve to be treated fairly. Correspondingly, the company should ensure that the alleged perpetrator is given a copy of the complainant's statement – and assured that they will be given the right of reply. At this point, it is an allegation and not fact, so the alleged perpetrator needs to be approached with sensitivity and tact and supported throughout the process in the same way the complainant is.

Conducting a workplace investigation

Depending on the complexity of the matter, a workplace investigation may be the logical next step in determining the facts of the allegation. Conducting a workplace investigation requires a certain level of skill and training, and there are some good reasons why a HR department might consider outsourcing this to an external provider. Complex investigations which might ultimately lead to a dismissal may be best handled externally. Investigations must be fair and thorough, and this takes time. In today's HR departments, HR professionals are often already maxed out, and this can cause investigations to be delayed or incomplete. An investigator also needs to be impartial and unbiased, and the best way of knowing this for certain is by looking to an external provider. There are a number of steps which must be taken and everything must be documented in case the investigation is ever reviewed by an external party. That also requires having someone who knows how to create an investigation file and report that will withstand external scrutiny.

Ultimately, management will decide whether or not to uphold the complaint. If the complaint is upheld or if the complaint is found to have been maliciously made, then the issue becomes a disciplinary matter. And that's a whole other ball game.

Investigating Employee Fraud

Research undertaken by Mazars Ireland shows that Irish businesses are experiencing financial loss due to occupational fraud and abuse. Of the senior business leaders surveyed by Mazars Ireland, approximately 50% had experienced a loss due to occupational fraud and abuse over the past two years, with the average financial loss being between €10,000 and €20,000.

Ideally employee fraud, for example, financial irregularities or theft, would not happen. And employers can work to prevent such fraud through a variety of methods. For example, employers can strive to ensure that their employees are engaged – where employees intuitively think of the organisation's welfare rather than simply viewing their employer with mercenary intent. More engaged employees are less inclined to commit fraud. Because they are heavily invested in their employer's welfare, they strive to do what is best for their employer.

So – prevention is better than cure. But if prevention fails and a fraud may have occurred, then what should an organisation do? Because employee fraud does happen! You may, for example, remember the case of John Rusnak. He worked for an American bank in which AIB had a majority interest. He was a currency trader – first losing his employers millions through bad judgement – but then committing fraud through trying to cover up further trades and losses. The losses totalled $691 million!

Obviously, the Rusnak case is an extreme case. But, by definition, every incidence of fraud is a drain on profitability and carries with it the risk of reputational damage. And the financial cost of fraud goes beyond the loss both from the fraud itself to include investigation, management time and potential prosecution.

How an organisation deals with an incidence of fraud can range from minimising

their losses to exacerbating the situation. Of the senior business leaders surveyed by Mazars Ireland, approximately 34% of respondents reported that they did not have formal investigation procedures or anti-fraud policies in place and rely heavily on internal audits to catch such crimes.

Ideally when such issues occur the employer will recover their assets and protect their reputation. However, care needs to be taken not to break the law and leave the organisation liable to prosecution by an aggrieved employee. Employees have a right to privacy. But employers have a right to protect their organisation. It's a delicate balancing act. Employers are also now legally mandated to protect employees who have raised concerns over potential wrongdoing by others in the workplace. The Protected Disclosures or Whistleblowing Act of 2014 became operational on July 15th 2014 and is intended to follow international best practice on whistleblower protection.

Should a company always investigate a fraud – or even a suspected fraud? There is a cost to investigations. But there are also benefits to carrying out an investigation. Most obviously there is the potential of uncovering and stopping the fraud. There is also the benefit of setting a visible precedent – that the company takes fraud extremely seriously. And of course, there is the potential to rid the organisation of the fraudulent employee – thereby eliminating the risk of recidivism by that particular person.

If a company decides to investigate, then who should do the investigation? The investigation must be unbiased, and the people appointed to carry out the investigation ought to be trained and skilled at carrying out such investigations. A team would normally be established – and could include a HR professional and a senior manager.

Many organisations have trained their own managers to carry out investigations, but they will invariably be guided by HR professionals and employment law solicitors. A knowledge of current employment legislation is crucial – it would be counter-productive for an investigation to run awry of employment legislation, for example, by impinging excessively on the suspected employee's right to privacy.

Speed in investigating fraud is valuable – the speed heightens the chances of detection and reduces the potential loses. And it is also highly desirable for someone on the investigation team to have reasonable knowledge of the subject matter.

Depending on the nature, severity and extent of the alleged fraud, an investigation could involve a number of departments. This often includes finance – perhaps with the help of an external forensic accountant. If IT equipment needs to be examined, an IT expert may need to be involved. Perhaps the Gardaí may also be involved.

However, if the Gardaí are involved, control of the investigation may be ceded to them. This could be problematic. The employer may not agree with the direction or nature of their investigation. Additionally, the employer's case may not be as important to the Gardaí as it is to the employer. The pace at which the Gardaí investigation will proceed is subject to its place among all the other cases that they are dealing with. The Garda Bureau of Fraud Investigation "is not in a position to investigate every referred case of

suspected fraud. For optimum resource utilisation, investigations are focused on major and complex fraud".

It is important therefore that the employer carefully weigh up the level and extent of the suspected fraud and proceed cautiously with the advice of a HR professional, perhaps an employment law solicitor, and perhaps the Gardaí. It can be helpful to liaise with the Gardaí if only to ensure that the workplace investigation does not accidentally compromise a later prosecution. If fraud is proved to have occurred, then care is still needed before considering firing the employee. For example, there is the possibility that the employee, through a failing of the organisation, may not have known that the fraudulent activity was actually fraudulent. It is important to connect the fraudulent activity directly with one of the organisation's policies and procedures – this allows the organisation to be specific in its reasoning for terminating the employment.

Running a remote workplace investigation

A good starting point when considering conducting a remote workplace investigation is to outline clearly each of the steps you would take when conducting a traditional investigation. Perhaps you do not have a lot of experience, or it has been a long time since you completed one. Either way, it would be in your best interest to re-familiarise yourself with the process.

One of the very first items on your list should be to review the existing policy in place at your organisation. You are obliged to follow the procedure outlined, as it has already been established and agreed upon. If this policy mentions face to face meetings specifically, you may need to insert an addendum or an amendment to your existing policy in order to take account for conducting meetings remotely.

You should also provide all parties with the terms of reference that clearly outlines exactly what is being investigated and the scope of the investigation, and you will need to outline that the remote meeting is also expected to be confidential. That means that you need to prepare your employee in advance of how long the meeting is expected to take and that they will need to be in a private space throughout.

Setting a time and date for the interview is next, and all parties should be notified in writing. As this will be a remote meeting, you may need to offer your employee more flexibility than usual. Your employee may be dealing with children in the home and may not have access to a private space until a certain time of day. It therefore makes sense to ascertain their preferred time of day and week in advance of the meeting being set. Prior communication with them regarding their personal situation will help to make finalising a date much more efficient.

Usually parties are summoned to a dedicated private space, in the workplace or perhaps in an external venue if enlisting the help of a third-party HR consultant. When running a remote investigation, your meeting must take place online. In these cases, ensure that you have set up a dedicated meeting room that is password protected for security. Use an established and well-known provider that complies with privacy regulations (more in Part Two of this two-part series Link). If conducting multiple interviews, you should

ensure that you are using unique links for each one, rather than setting up one meeting and just relying on people to only log on at the time requested. Alternatively, most providers will offer a 'waiting room', or a 'knock to enter' policy, so make sure you adjust this setting to minimise the risk of having any interviewees turning up announced. This link should be sent to attendees via email when arranging the interview, or steps on how to access the meeting should be clearly explained in the notification letter. Remember that if your attendee wishes to include a representative, that representative will also need to be provided the details.

Best practice in HR matters – if viable for your business – is to separate out the process, meaning that the person who conducts the interview should be different to the person who decides the outcome. That means that you should also ensure that your colleagues in the HR department are up to speed with the tech platforms needed to conduct the investigation – and that you provide access to training where necessary. You can even record a short video and screen share to show how to perform certain steps in the process and then send it around to each of your colleagues that will be involved. Similarly, it would be in your best interest to send your employee directions on how they can access the meeting. Although many of us have become acquainted with online video conferencing tools of late, this should not be taken for granted. The last thing that you want is to be fully prepared for a meeting only for it not to go ahead because your employee was unaware that they would need a certain browser to access the link, for example. Sending your employee a brief video explainer will help minimise this possibility. It is also worth reminding them of video calling etiquette, for instance making sure that they are in a well-lit room and that they have informed those they live with that they should not be disturbed.

Using the right tools

Choosing the best platform to suit your needs may well seem challenging. There is a running joke about online meetings being frustrating. However, technology has come on in leaps and bounds since the first video conferencing software was rolled out. There are many different providers that offer all kinds of functionalities. You may opt to buy licences for an all-singing all-dancing platform that can be used in other areas of the business. Or, you may choose to have a separate tool. Either way, there are a few features that yours should have:

- The ability to invite multiple participants to the same meeting in case your employee opts for representation
- The ability to record the interview for transcription purposes
- The ability to make the meeting password protected and add a waiting room or knock to enter option
- The option to extend an interview past its scheduled time automatically

Zoom is one tool that has been recommended due to its ability to record high-quality video and audio, though you will need to purchase a subscription should you wish to use it, as the free version disconnects meetings automatically after 40 minutes. In order

to access the full functionality of Zoom, your interviewee will need to download the app in order to be able to access the meeting. This can lead to delays, and your interviewee is within their rights to refuse to download the application. If they wish to access the meeting without downloading, then they will need to open a free account using an email address and password.

At Insight HR, we have been using Microsoft Teams as it suits all our needs currently. We can invite multiple participants to each meeting, record meetings, and there is a waiting room (or lobby). It also does not kick us out of the meeting once the calendar scheduled time has passed.

Having a backup Dictaphone or even normal phone recording in case the software fails is also advisable – though this should only be done from a work specific device for security purposes.

Whichever platform you decide to go with, it is strongly advised to trial the platform – and the recording – in advance. You may be well used to different video conferencing platforms. However, in a workplace investigation, the stakes are considerably higher. You really want to leave no room for error. Technology can fail at the most inopportune of times – and often does! So, testing the platforms beforehand is key.

Data privacy

In May 2018, GDPR came into effect across the EU. It is designed to protect individuals' personally identifiable information by laying out very specific rules on the types of data allowably collected by organisations, how that data should be treated and how long it should be stored for. It outlines six principles that data controllers must adhere to when collecting data. Avoidance of the guidelines may lead to a data breach, a complaint being made to the Data Protection Commissioner, and ultimately a heavy fine for your business.

Given that the GDPR was introduced three years ago, you have probably already familiarised yourself with its stipulations. However, with remote working comes the increased risk of data breaches, and any organisation with remote workers will need to take some additional steps to ensure the ongoing security of personal information. While this is true for all departments across the business, it is especially true for the HR department, as this is the department which usually collects employees' personal information such as home address, phone number, data relating to salary and performance reviews and sensitive medical information.

When dealing with sensitive matters such as an internal investigation, the last thing that you need is for security to be compromised. You also need to think about what kind of consents you may need from your interviewee. It is vital that you give careful consideration to the following items.

Data storage

Are you storing the data relating to the investigation on a workplace network drive accessible via a VPN? Is this drive separate to the company-wide one? Who has access rights, and why?

Are you storing data locally, in a desktop folder? Have you password protected this folder – and your device?

Do you have paper files relating to the investigation? If so, where are these currently being stored? If you live with others, how are you ensuring the privacy of these files?

If you have been taking notes on a notepad, what type of information do these notes contain? Where is this notebook being stored?

Is the investigation data currently stored in multiple locations? If so, why? Can you consolidate the data?

Third party providers

What are the different apps/tools you need to use in order to conduct your investigation? (This includes not only your video conferencing tool but also any other tools being used, such as OneDrive or Google Drive for file storage)

Do they have a robust privacy policy and GDPR statement?

Where does the provider store any recordings or files, and how long do they store them for?

Have you thoroughly researched the providers reputation for data security?

How many people in your company have access to the provider's account that you will use for the investigation?

If using a video conferencing tool that allows all parties to record, do you need to implement extra measures to ensure that your interviewee does not record the meeting?

Data Consents

Has your interviewee consented to the use of a third-party tool for interviewing purposes?

Does your interview consent form allow for the meeting to be recorded? Additionally, if your software records both video and audio, has your interviewee given their consent to have their image captured, as well as their voice?

If your interviewee wishes to include a representative, have they also signed a consent form?

Has your interviewee signed something in which they acknowledge that the investigation should remain confidential? Are they aware of any measures they might face should they breach this?

You likely have received direction from your IT department regarding general IT security when working from home. Make sure that you have implemented all measures suggested by them, especially if using your own device rather than a dedicated work device. Use a password generator, and a storage system such as KeePass that will keep all your passwords secure. Remain alert when it comes to phishing emails. Test yourself

to see how easy you find it to identify a phishing email here https://www.phishingbox.com/phishing-test

Ensure your anti-virus software is up to date and you are regularly checking for updates, especially if you use your own device at all. Install an AdBlocker, or ask your IT department to install one for you. You can also install a DNS filter, such as this free version https://www.opendns.com/home-internet-security/

Practicalities

The interviews should always be conducted in a private, confidential manner. Although we are big advocates of remote working and hugely supportive of those that need to work while also minding children, this is not the time for your partner/housemate/child to come bursting into the room. It is your responsibility to safeguard against this as much as is possible. Explain clearly beforehand the importance of privacy for this meeting. Try hanging a sign on the door to mitigate the risk of them walking in unannounced. Another good practice is to sit with the back of the laptop facing the door. That way, even if someone comes through the door you will have a chance to address them before they see your video screen and your interviewee.

On that note, your equipment should be suitable for the interview. Headphones should be worn as this minimises the possibility of anyone else but you hearing the statements. Ensure your computer is automatically checking for updates and that these have all been done before the interview. Sign into your chosen software at least ten minutes in advance so that you can rest assured it is working. Internet speeds can be assessed beforehand if you wish – a simple Google search will bring up a free speed checker.

While you need to ensure all your equipment is up to date, you also need to run an assessment on your employees' technology. What happens if they cannot download the software? What if they do not have a stable internet connection or any at all? What if they do not own a personal computer? If feasible to do so, your organisation may wish to supply needed equipment to your interviewee in order for them to complete the interview. Even in this day and age though, we can't expect everyone to have the familiarity with technology that is required for video conferencing. In these cases, how are you facilitating the interview? Will you be able to do it via phone call and record it? Being prepared for every eventuality will help make this process less stressful.

If you need to transfer the video recordings to be transcribed, then ensure you are using a secure file transfer platform. Due to the size of video recordings, you will likely not be able to send via email. Whatever you do, don't be tempted to upload to your personal Drive and share a link. Re-read the above section on data privacy if still unsure.

Be realistic

Workplace investigations are a sensitive subject that can be a potential minefield for employers. They can be tricky to get right, even in non-pandemic times. However, they must be completed effectively, efficiently, and fairly. Despite your best efforts, you may find it much easier to outsource the investigation to a trusted third party. Be realistic in your abilities, but also your resources. If you are the only HR Manager in your

organisation, and you are dealing with a complex matter, then you will need to look externally for support so that you can provide a fair process to all involved.

Writing the investigation report

An investigation report is a record of the investigation process from start to finish. It documents how the investigation was conducted and the findings of the investigation. Its purpose is to thoroughly explore the particulars of the incident upon which the investigation is based, examine all related evidence, and provide the necessary detail for the deciding party to determine whether a wrongdoing has occurred. It also enables the decision maker to decide on the appropriate course of action. It may end up being used as evidence in legal proceedings.

Even for weathered HR professionals, writing an investigation report can be intimidating. It is important that the report leave no room for ambiguity. It should be written using clear, concise language. It should also read easily, without flowery language or variations in writing style. Consistency is key. Authors who write excellently otherwise often struggle with this when compiling a multiple-page report over a number of days, as they are more concerned with accurately scribing the facts of the investigation. However, giving prior thought to the writing process helps to create a professional and credible report that has been given due consideration.

Considering the following before you write the report is advised. If there are multiple contributors (i.e. authors, editors, proof-readers, fact-checkers), then create an easily accessible document in which you can make a written note of any style decisions if needs be. This way, you can ensure that your team is maintaining a consistent style and flow to the document as they update it.

Point of View

One of the most important style decisions that you need to make is from whose point of view the report will be written. The two most common point of views in investigation reports are first person and third person. The difference between them is that when writing in the first person, you will be writing as yourself. Therefore, you will be using the phrase 'I found' rather than 'the investigator found', the latter example being written in the third person. Though many legal documents are written in the third person, HR professionals may decide to write a report in the first person. Neither is necessarily preferred over the other, however, it is important to choose one style and stick with it so as to minimise confusion for the reader.

Titles, Names, Dates, Times, Numbers and Quotations

How are you referring to the parties that feature in the report? Are you calling them by their first name? By their full name? With the use of Mr. and Mrs.? Are you referring to them by their roles in the report (ie Witness 1, the Complainant etc.)? How about job titles – are you capitalising them? Do you include everyone's job title in the body of the text each time you write their name? Deciding on this beforehand will help you to

remain consistent throughout the report. As a recommendation, we advise including a list of all parties, their full names and job titles in the opening pages of the report. As the parties are introduced within the body of the report, we recommend including their full names and job titles the first time they are introduced, with a note to inform the reader how they will be referred to 'hereafter'. At Insight HR, we usually use a party's last name with the preceding Mr. or Mrs. However, be careful of similar names. Including the first initial of a party who shares their surname with another party is advised.

An investigation report often makes references to dates of incidents. How are you writing these dates? Are you using the numerical style, or are you writing the dates out in full? If using the numerical style, are you using dashes or slashes? There is not necessarily only one correct way to present dates in an investigation report, however there should be only one choice made and stuck to throughout. The same goes for time. How are you reporting specific times? Are you writing them out in full? Are you using the numerical style, with am and pm? Are you using the 24-hour style?

Another vital decision to make regards the use of quotation marks. Decide whether you wish to use a double set or a single set. This is very important, as often investigation reports can include quotations of quotations. In this instance, you will be using both styles. For instance, the passage may read as such:

Mrs. Kelly stated that "Mr. Byrne said, 'you haven't swept the floor' and I replied 'I was told not to'".

This may seem like an obvious distinction between quotes. However, it can become confusing if the author is not consistent in their use of quotation marks and there are a lot of quotes included in the report.

These are just some of the important style decisions to make prior to putting the report together for the sake of consistency and good flow.

Diction

Diction refers to the choice of words used to create a particular effect, for instance formal language vs informal. For an investigation report you will be using formal language. However, formal language may still include colloquialisms and jargon. Different industry sectors often use terms, phrases and expressions that are only obvious to those operating within that sector. For example, an IT company may use technical terms that are not self-explanatory. Before composing your report, critically review the likelihood of this type of language finding its way into the report, especially contained within quotes from witness statements, and decide on how it will be treated. Will you insert an explanation in brackets after each instance? Is there a need to provide an explanation of key terms in the opening pages of the report? Deciding on this prior to starting your report will save you time in the editing process.

Another important point to consider is the unconscious meaning that certain words carry. Consider the use of the word 'admit'. The dictionary definition of this word is 'to confess to be the case'. It may then seem like an appropriate word to use in the investigation report to describe something contained within a statement. However,

given its common use in courts of law, it now carries certain connotations of guilt and intention to conceal that can therefore provide an impression of a party which may not necessarily be accurate. That is not to say that the word should not be used in the report. It should, however, be used sparingly. Choosing another word, such as 'confirm' may be more appropriate. This is just one such example – there are plenty others. It is human nature to express oneself in emotive language. Witness statements may therefore be full of words that carry certain connotations. As an investigator, it is best to not overuse this type of language, instead reserving it for including only within direct quotes.

Where to go for further help

If you need to run a workplace investigation, remember that it needs to be fair and impartial. The best way to achieve this is by enlisting the help of an experienced third-party provider.

At Insight HR we have over twenty years of experience running workplace investigations. Our head of workplace investigations is an ex-Guard, which gives us a unique vantage point. Our HR consultants have wide and varied experience and can hold your hand as you navigate this tricky road.

Call us for a confidential discussion on 0567701060, reach out to us via email, social media or via our website.

Insight HR has you covered.