EMPLOYMENT TRIBUNALS

Claimant: Mr P Lloyd

Respondents:
1. Marston Holdings Limited
2. Marston Recourses Limited
3. Marston Group Limited

HELD AT: Liverpool **ON:** 6, 7 & 8 August 2019
22 August 2019 (in chambers)

BEFORE: Employment Judge Shotter

REPRESENTATION:

Claimant: In person
Respondent: Ms L Kaye, Counsel

RESERVED JUDGEMENT

The JUDGEMENT of the Tribunal is as follows:

1. The correct name of the respondent is Marston Holdings Limited, the claimant's employer and the claims are dismissed in their entirety against the second and third respondents who longer have any interest in these proceedings.

2. The claimant did not suffer an unlawful deduction of wages and offered no evidence in respect of this claim, which is dismissed.

3. The claimant was not unfairly dismissed, his claim for unfair dismissal is not well-founded and is dismissed.

REASONS

Preamble

1. In a claim form received on the 11 September 2018 following ACAS early conciliation between 23 July and 23 August 2018 the claimant complained that he had been unfairly dismissed on the 7 June 2018 for five counts of misconduct which,

he believed, there was no evidence of and the respondent was in breach of the ACAS Code of Practice. The claimant also maintained that the respondent had failed to take into account mitigation, including the fact he had not received training, his unblemished record, and the decision did not fall within the band of reasonable responses. The claimant also claimed for notice pay by way of a wrongful dismissal complaint and unlawful deduction of wages that were unparticularised and for which no evidence was put forward.

2. The respondent denies the claimant's claim of unfair dismissal on the basis that the claimant had breached its policies and procedures, the contractual implied term of trust and confidence and the decision to dismiss fell within the band of reasonable responses.

3. The Tribunal heard evidence from the claimant on his own behalf and on behalf of the respondent it heard Lee Lovatt, on street audit manager and the claimant's line manager, David Fenwick, risk framework business partner and dismissing officer, and Deborah Cooper, group organisational development director and appeal officer. The Tribunal found the respondent's witnesses to be credible and cogent, it found the claimant was not credible and gave contradictory and conflicting evidence as set out below.

Agreed issues

4. The issues were agreed between the parties from the outset of the final hearing as set out below:

Unfair Dismissal

1. The parties agree, the Respondent relied on conduct as reason for dismissal, a fair reason within the meaning of s.98(2)(b) Employment rights Act 1996?

2. Did the Respondent act reasonably in the circumstances (having regard to the size and administrative resources of the Respondent) and in accordance with equity and the substantial merits of the case, in treating conduct as a sufficient reason for dismissing the Claimant (s98(4) Employment Rights Act 1996)?

    a. Did the Respondent hold a genuine belief in the claimant's misconduct namely:

        i. Downloaded, loaded or used authorised pirated software/video files on company PCs;

        ii. Sent inappropriate material to private email addresses in contravention of policy which may represent a disclosure of confidential information;

        iii. Installed software without IT authorisation;

        iv. Used the TOR browser which has the potential to hide internet activity from the company in the absence of a requirement by R to do so;

v. Used netplwiz.exe which has the potential to change access rights without authorisation.

The Claimant asserts, DF did not hold a genuine belief in his guilt because he failed to consider all available evidence including C's written defence document which was ignored.

b. Did the Respondent have reasonable grounds for its belief that the Claimant behaved as described at paragraph 2(a)?

The Claimant asserts the Respondent did not have reasonable grounds for its belief, because the Claimant did not receive training in the applicable IT policies and procedures by LL, DF and the Head of Department.

c. Did the Respondent conduct a reasonable investigation into C's misconduct?

The Claimant asserts LL conducted a limited and ineffective in that he:

i. Filtered the evidence;

ii. Falsified the evidence;

iii. Misrepresented the evidence in the Investigation Report;

3. If so, did the decision to dismiss fall within the band of reasonable responses open to a reasonable employer in the circumstances?

a. The Claimant asserts the decision was outside the band based on the evidence available because:

i. The 7Elements reports was asserted as true in the investigation and the disciplinary hearing;

ii. The C's written defence (counter-evidence) disputed the accuracy of the 7Elements reports, and the conclusions drawn;

iii. LL falsified, filtered and misrepresented evidence in the Investigation report;

4. Has the Respondent followed a fair procedure?

a. The Claimant asserts the procedure was unfair because:

i. C was invited to an investigation meeting on 19th April 2018 without notice;

ii. C was not advised he could be accompanied to the investigation meeting on 19th April 2018 as per R's policy;

iii. C was not told he was under investigation;

iv. C was not told who instigated the investigation;

v. C was not provided with the meeting notes of 19th April 2018 following the meeting;

vi. C was not asked to sign the meeting notes of 19th April 2018 to confirm their truth;

vii. C was not advised he could be accompanied to the investigation meeting on 9th May 2018 as per R's policy;

viii. C was not provided with the meeting notes of 9th May 2018 following the meeting;

ix. C was not asked to sign the meeting notes of 9th May 2018 to confirm their truth;

x. DF failed to read the written defence prior to the disciplinary hearing;

xi. DF failed to address the contents of the written defence in the disciplinary hearing;

xii. DF failed to establish the essential facts in the disciplinary hearing;

xiii. DF failed to consider the mitigating circumstances – the Company failing to provide me with the IT policies and training in relation to those policies (Acceptable Use, Information Security Brochure);

xiv. DC failed to address LL's motives as highlighted by C (in the appeal letter) in the appeal hearing;

xv. DC failed to address all points of appeal in the appeal hearing including the lack of consideration by DF of C's written defence and the lack of training as mitigation;

xvi. DC failed to address all points of grievance in the appeal hearing;

5. If the Claimant is successful, to what remedy is he entitled?

i. Is it just and equitable to reduce any compensatory award (s.123 Employment Rights Act 1996?);

ii. If the Tribunal finds that a fair procedure had not been followed, would the Claimant have been dismissed been if that had not been the case (Polkey v AE Drayton Services Limited [1978] ICR 142)?

iii. Did the Claimant cause or contribute to his dismissal and if so, by how much?

iv. Should there be an uplift for a breach of the ACAS Code of Practice and if so, at what level?

Wrongful Dismissal

1. Did the Respondent dismiss the Claimant in breach of contract entitling him to notice pay?

2. If so, what notice pay was C contractually entitled to?

Submissions

5. The claimant produced a 9-page list of issues on the 13 August 2019 without the consent of the Tribunal or knowledge of the respondent. The Tribunal provided a copy for the respondent's observations which are set out below. The claimant's explanations how he came to produce a second set of reasons raised fundamental issues as to his credibility. In a separate letter of the same date the claimant justified his actions citing the following reasons:

5.1 "As a litigant in person, I was originally unaware of how both written and oral submissions should be made until the Respondent's barrister showed me by example…

5.2 I was given an additional 20 mins to quickly write some oral submissions on the last day of my tribunal and thought this would be a more acceptable format to present my written submissions in…

5.3 As Judge Shotter stated she would make her decision on the facts of the case and the facts alone, these new written submissions simply reflect my oral submissions and signpost facts which may not have been covered in the time allotted for my cross examination compared to the 5.5 hours afforded to the Respondent to cross examine just me".

6. The respondent objected to the claimant's additional written submissions in a letter dated 15 August 2019 giving the following reasons with which the Tribunal agree:

6.1 "It is the Respondent's position that the Tribunal gave clear instructions after the final hearing for submissions that were handed in at the final hearing to be sent electronically. There was absolutely no permission nor suggestion that these submissions could or should be altered…

6.2 The Claimant has spent 4 days following the final hearing considering the Respondent's submissions and reframing and redrafting his case to fit the Respondent's defence. This is entirely inappropriate and it is the Respondent's position that the overriding objective (Employment Tribunal Rules of Procedure Schedule 1(2)) is to ensure that cases are dealt with justly and fairly...

6.3 It is also the case that some of the above new matters were not put to the witnesses for challenge and therefore there is no conceivable basis that the Claimant can rely on those matters as submissions, new or otherwise.

6.4 On day two of the hearing the Tribunal gave guidance as to how to prepare and present submissions. The Respondent's Counsel also assisted the Tribunal and the Claimant by assisting the Claimant and explaining that he may wish to make a bullet point list under the list of issues to give him a starting point with this task. It is the Respondent's position that the Claimant clearly understood the guidance provided by the Tribunal as he handed in written submissions, printed off case law and delivered oral submissions at the final hearing.

6.5 The Claimant handed in written submissions following an extended lunch break which was granted to him to allow him additional time to read the Respondent's submissions. It is therefore incorrect of the Claimant to say that he was given 'an additional twenty minutes to quickly write oral submissions' on the last day of the Tribunal. In fact, he was given an extended lunch break on day two to review the Respondent's submissions, following which both parties handed them in. Counsel for the Respondent delivered submissions orally and the Claimant was then granted some 25 minutes to review and prepare a response to the oral submissions…

6.6 The Respondent would like to clarify that the Claimant was given 1.5 days to cross-examine the Respondent's witnesses. After each witness's evidence, the Claimant confirmed that he did not want to put additional questions to them. The length of cross-examination of the Claimant was caused, at least in part, by:

1. Questions having to be repeated or put again, sometimes multiple times; and
2. the length of the Claimant's responses."

7. Tribunal has considered the claimant's and respondent's arguments and notes the following as recorded in writing by the Judge during the hearing, it has taken time to read the claimant's additional submissions which it does not intend to deal with in any detail whatsoever but has taken into account:

7.1 The claimant made an application to introduce into evidence confidential documents marked C1 to C3 that were not relevant to the issues, the claimant conceding that he had sent the confidential information from work to his private email address. There was no need for the Tribunal to view the confidential information, especially since the claimant "only realised C1 and C2" were not confidential when he had consulted ACAS and not during the disciplinary process and thus it was not a matter argued before the disciplinary or appeal officer. It is notable in relation to C3 the claimant accepted it was confidential and he "chose stupidly" to send them to his personal email address. It was agreed the front sheet of C3 was put into the evidence for cross-examination purposes, as this did not include confidential information irrelevant to these proceedings.

7.2 The claimant's application was completed by 11.15pm and the case adjourned to 2pm for the Tribunal to read, the parties agree the issues, which they did, and for the claimant to finalise his questions on cross-examination in the light of those issues. The claimant was made aware that respondent's first witness was Lee lovatt.

7.3 The claimant cross-examined Lee Lovatt from 14.07 to 16.30. He had difficulties moving from an issue which he considered to be important and key to his

defence, namely Lee Lovatt's motivation and asked irrelevant questions, despite the Tribunal's guidance and counsel's objections. The claimant stated he had spent 3 to 4 weeks preparing his cross-examination of the respondent's witnesses. An agreement was reached as to the amount of time the claimant would spend cross-examining the respondent's remaining witnesses and the time allocated for the claimant's cross-examination given the very serious possibility that the case would go part heard with the earliest re-listing in October 2019.

7.4 The second day of hearing commenced at 9.30am and the claimant, who reported he had been up until 3.30am sorting out his cross-examination questions, proceeded to cross-examine Lee Lovatt until 10.54.

7.5 Cross-examination of David Fenwick, the dismissing officer, commenced at 11.10am and finished at 12.34 when the claimant indicated he had no further questions on being asked this question by the Tribunal. On hearing this the Tribunal pointed out David Fenwick., as the dismissing officer was a key witness, and asked the claimant if he was sure he had no further questions to which the claimant responded "I've looked at the agreed issues. I've covered the points…If I question him further it will do more harm to my defence than good. The main points I wanted to get across was that my written defence was not considered, failing to consider mitigating circumstances of the company failing to provide IT policies and procedures and failing to establish the facts in the disciplinary hearing." In addition to re-examination by counsel, the Tribunal asked a number of questions for clarification purposes which took David Fenwick's evidence to 1.11pm.

7.6 The claimant requested an extended lunch period of 1.5 hours in order to prepare his cross-examination of Deborah Cooper. Additional time was granted at the claimant's request and cross-examination commenced at 2.55pm and finished at 16.50.

7.7 On the third day of the hearing the claimant's cross-examination commenced at 10.08am and following a number of breaks including the lunch, during which it was agreed the claimant would be provided with a copy of the respondent's written draft submissions in order that he could respond to it in his own submissions. The claimant indicated he had prepared written submissions.

7.8 Following the lunchtime adjournment, the cross-examination of the claimant commenced during which he alleged "I wasn't given the time and leeway to question Mr Lovatt in the way I wanted…I don't believe I had the time allotted to me" when a question on cross-examination put to him by counsel hit the mark. The claimant's allegation was explored with both parties, and counsel reminded the claimant and Tribunal that (a) he had put many irrelevant background questions to Lee Lovatt, and (b) the Tribunal had asked after each of the respondent's witnesses cross-examination for confirmation that the claimant had put all his questions, and he confirmed that he had.

7.9 Cross-examination of the claimant finished at 16.29 at which point he acknowledged where he was uncertain as to the question asked, the Tribunal

asked counsel to re-question and re-clarify, which she did. The Tribunal notes there were a number of occasions when this took place. It is notable the claimant took approximately 30 minutes to then clarify his case during which he confirmed the TOR browser could be used to search the deep dark web to commit criminal offences, and that he had used it 25 to 30 minutes "within a short time of starting it," did not find it suitable and it became "just another browser" on his laptop. When the Tribunal asked the claimant why he felt the dismissing officer held a genuine belief that he had committed an act of gross misconduct by down loading and using the TOR browser the claimant's response was "the explanation I gave was given no credence as a possible explanation…I don't think they believed me…" and therein lies the nub of the claimant's case, and the reason why the claimant's oral and two sets of written submissions (both of which were considered by the Tribunal), his arguments on motivation and further investigation, do not assist him.

7.10 The claimant was given between 17.34 to 6pm to consider the respondent's oral submissions having originally requested 10 minutes. The claimant referred to written submissions and took until 6.20pm. The hearing finished 6.30pm with judgment reserved due to the late hour. The claimant gave no indication he was unable to put forward all of his submissions, having been given an agreed 30 minutes in which to do so, he finished in 20 minutes.

7.11 The claimant's submissions essentially followed the observations set out by the Tribunal below, who does not propose to deal with them line-by-line in light of the overriding objective. It is notable that he raised a number of matters not previously put to the respondent either during the disciplinary process or on cross-examination at this liability hearing, for example, a suggestion that he should have been re-trained as an alternative to dismissal.

8. The Tribunal was referred to an agreed bundle of documents and having considered the oral and written evidence and oral and written submissions presented by the parties (the Tribunal does not intend to repeat all of the oral submissions, but has attempted to incorporate the points made by the parties within the body of this judgment with reasons), it has made the following findings of the relevant facts.

Facts

9. The respondent employs 5000 people in 250 locations within the UK and it holds a substantial amount of confidential information, including personal data as part of the enforcement and debt recovery arm in the business. Its clients include the Ministry of Justice.

10. The claimant was employed by the respondent as a 'On-Street audit and Fraud Investigator' based at Helmshore. He had previously worked in a different role within the respondent on a self-employed basis.

11. The respondent has a number of policies and procedures posted on the intranet available for employees to access and read. In addition, it regularly sends to employee's memorandums attaching copies of policies and procedures confirming their availability.

12. The claimant received a Memorandum on 27 January 2015 which he signed on the 3 February 2015 during induction. The Memorandum listed a number of policies and procedures including disciplinary and whistleblowing clearly stating, "Copies of all policies and procedures are available on the intranet, HR or the line manager." The claimant was not provided with a hard copy of the Staff Handbook, however, he had access to it on the intranet and was aware of this fact. The claimant chose not to read the respondent's Policies and Procedures, and did not take the trouble to understand the contractual terms he was bound by, having merely glanced at the contract. No reference was made within the body of the Memorandum to a 'Group Acceptable Use Policy,' However had the claimant taken the trouble of accessing the policies and procedures on the internet and then read the polices, the Group Acceptable Use Policy would have been available for him to access and read. The claimant's view was that employees were not required to read in any great depth their contracts or view and read the policies and procedures, and it was unrealistic of the respondent to expect this. The respondent did not agree.

Employment contract

13. The claimant was issued with Terms and Conditions of Employment signed on 3 February 2015, his employment having commenced on 12 November 2015. The Tribunal is satisfied the claimant would have been aware of the raft of policies and procedures issued by the respondent and available on the intranet. It did not accept as credible the claimant's evidence given during this liability hearing which conflicted with that given to the respondent during the disciplinary process, that he was not informed of their existence when upon or after commencing his employment having previously worked for the responded as a self-employed bailiff for a number of years when he was granted a limited access on the laptop provided in direct contrast to the information accessible when carrying out his employment as a on street audit and fraud investigator.

14. The relevant parts of the contract are as follows:

14.1 Paragraph 13 titled "Summary Dismissal" set out a list of examples of gross misconduct that may lead to summary dismissal including "gross carelessness or neglect of duty risking serious consequences to the health and/or safety of any of the company's employees or to the company property and business reputation…**email or internet abuse**" and "any conduct which, in the reasonable opinion of the company, brings you or the company into disrepute" [the Tribunal's emphasis]. The claimant would have known from this clause that internet abuse covered accessing the deep dark web via a TOR browser and the hidden activity could not be traced by the respondent, was an act of gross misconduct.

14.2 Paragraph 14 provided "Other forms of misconduct that may result in a disciplinary procedure" included "misuse of working time, facilities, equipment… this list is not exhaustive. Other forms of conduct and omissions that could result in lowering the company's reasonable standards of efficiency and conduct are also covered by this clause."

14.3 Paragraph 17 provided a definition of confidential information that included "information relating to the business…or affairs of the company…includes (by

way of example only and without limitation) technical data, know-how, financial information, financial forecasts, marketing strategies and password and security information." The claimant would have realised that, had he properly addressed his mind to it, transferring confidential company information to his personal email address was an act of gross misconduct.

14.4 Paragraph 18 set out a confidentiality clause and 18.3 that "You must not at any tome make a copy of or record, summarise or precis any document or any part of a document belonging to the Company or record the same in electronic or other form except as may be specifically required for the purpose of your employment under this agreement.".

14.5 Paragraph 19 referred to the respondent's Data Protection Policy "as contained within the Policies and Procedures Manual" and by signing the contract the claimant agreed to abide by the provisions and confirmed he had read and agreed to comply with the respondent's Data Protection Policy.

14.6 Paragraph 20.1 confirmed in respect of email and internet usage "The email system and internet are directly concerned with the business of the company. The company reserves the right to…monitor and view all data sent…whether internally or externally…Any unauthorised use of…internet systems is a serious breach of discipline and may result in disciplinary action leading to dismissal, including summary dismissal…By way of example only, the company will not tolerate the use of the system for…downloading or distributing copyright information and /or any unlicensed software…" The claimant was aware that the respondent could monitor his internet searches, and downloading and using the TOR browser circumvented this" and it was an act of gross misconduct.

14.7 Paragraph 23.1 provided "the software used or developed by the company is confidential and must at no time be sued for any purpose other than that which or for which it is authorised…"

14.8 Finally, at paragraph 26 it was expressly provided that the Disciplinary Policy and Procedures available on the intranet, a manager or from HR was non-contractual in effect.

Staff Handbook: Employee Communications

15. The Staff Handbook included a policy 'Employee Communications" which placed the onus on employees to take responsibility for their internet and email use. that the claimant does not dispute. It provided the relevant information:

15.1 "**Internet access is monitored to ensure that employees are not visiting sites unrelated to their jobs**, and to ensure that you continue to be in compliance with security policies…. all information received from the internet should be considered suspect…**You must not download software from the internet unless specifically authorised by the IT department**" [the Tribunal's emphasis]. The claimant, had he read the Staff Handbook, would have known downloading the TOR browser was a breach of the Policy, and he did not need training to understand this provision.

15.2 "Any discs brought from home to be used on the company's system must be virus checked by the IT department first."

Acceptable User Policy

16. The respondent issued a 'Group Acceptable Use Policy' as an appendix F to the Handbook. The copy before the Tribunal was a second version dated 17 January 2017. When cross-examining witnesses, the claimant made it clear that he had never seen this document before. The Tribunal did not find this evidence to be credible in respect of the claimant's state of knowledge; he may have chosen not to read the respondent's policies and procedures but it does not automatically follow he was unaware of their existence on the intranet. The evidence before the respondent during the disciplinary processes was contradictory with the claimant both denying and accepting he was aware of the existence of policies an procedures on the intranet as explored further below.

17. The aim of the policy was to ensure security incidents and breaches of confidentiality were minimised. Reference was made to the "organisation's information processing facilities shall be used in accordance with specified and published polies and procedures. The Policy, like all the others, was available for employees to access on the respondent's intranet. The relevant paragraphs are as follows:

17.1 "Directors, managers, team leaders and supervisors shall provide staff with education and training to support adherence to this Acceptable Use Policy…**All line managers shall be responsible for implementing the Acceptable Use Policy within their area of responsibility.** All staff provided with the organisation's information processing facilities shall comply with this Acceptable Use Policy" the Tribunal's emphasis.

17.2 "**The organisation's information shall not be processed on privately owned computers or remote access gained to company serves via privately owned computers**…Failure to adhere to this Acceptable Use Policy will increase the risk of information security breach for which they shall be held responsible and which may lead to disciplinary action."

17.3 "Staff with laptops who connect remotely shall be responsible for maintain and updating their malicious software controls on a weekly basis by following the instructions issued by the IT department."

17.4 "Staff shall report…significant software malfunction…to their immediate line manager, IT, compliance team." An email link was insert for access to the compliance team.

17.5 Non-compliance with the Acceptable Use Policy "may lead to disciplinary actions."

The respondent's Disciplinary Policy and Procedure

18. The Disciplinary Policy under the heading "General rules" provided confidential information must not be disclosed at any time. The following is relevant:

17.1 "No disciplinary matter will be taken until the matter has been fully investigated…at every formal stage employees…can be accompanied." It is not disputed between the parties that an investigation was not a formal stage of a disciplinary procedure, and the Tribunal agreed.

17.2 Examples of gross misconduct included "**downloading or use of unauthorised or pirated software on company PC's** or other action likely to allow a virus on to the system…the authorised disabling of software and/or anti-virus software…downloading or sending of inappropriate material in contravention of the System computer Access and information or Security Policies…**Breaches of confidentiality prejudicial to the company, breaches of confidentiality/security procedures**…" [the Tribunal's emphasis].

17.3 Under the heading "the formal procedure" reference was made to an "initial investigation including an investigation meeting and "if it is considered there is a case to answer a disciplinary hearing will be arranged "with a minimum of 48 hours' notice in writing. The claimant conceded on cross-examination that the formal procedures relates to the disciplinary procedure only, and the Tribunal took the view on a common-sense interpretation an investigation did not form part of the formal procedure to the effect that written notice of an investigation meeting was not required.

Employee Communications Policy

19. This Policy was also on the intranet and it was made clear that internet use would be monitored. The relevant clauses are as follows:

19.1 "You must not download software from the internet unless specifically authorised to do so by the IT department…

19.2 "You may not send personal emails or permit them to be sent on behalf of the Company, any email, attachment or posting which…contains information that is commercially sensitive or may have legal implications for the company…"

Group information Security Brochure version 2 2017

20. Appendix B to the Group Security Brochure provided employees must not, to protect their PC or laptop "download and install software yourself, always get the IT department to do it." Compliance with Data Protection was referred together with the employee's obligation to "take great care of all information…"

The claimant's employment and installing the TOR browser

21. The claimant commenced his employment working from the Helmshore office, having been contracted for 9-years previously as a self-employed enforcement agent by the respondent. During his time with the respondent, both as an employee and self-employed, the claimant received training on a wide range of matters including information security, data protection and on 27 March 2017 data protection and the information security system. It is not credible the claimant was unaware of the respondent's policies and procedures referred to above available for him to read on the intranet, and there is a difference between awareness and consciously taking the decision not to read the policies, which the claimant did.

22. In December 2014 the claimant installed a 'Start TOR browser' ("TOR browser) without informing the respondent of this at any stage, and the fact that the claimant had downloaded the browser was brought to the respondent's attention when it changed its IT provider. It is undisputed the TOR browser enabled the claimant to access the internet anonymously without leaving any trace of his visits to websites, allowing him to surf the web without the respondent being able to carry out any surveillance into his activities, which could not therefore be monitored. It is undisputed the TOR browser enabled the claimant to access an area of the internet known as the "deep dark web" and is used by criminal's and paedophiles to avoid detection in addition to the police, military and journalists as explained by the claimant.

23. The claimant's evidence that he was unaware installing the TOR browser software required authorisation from IT was not credible, as was his evidence that Lee Lovett's alleged reference to claimant's computer being "de-regularised" gave the claimant carte blanche to do what he wanted without reference to the respondent including IT, was not credible. In support of this proposition the claimant related how Lee Lovatt "oversaw" the installation of pieces of software "without making any comment whatsoever." It is undisputed the claimant did not make Lee Lovatt aware that he had installed the TOR browser, and it is disingenuous of the claimant to infer no comment would have been made had Lee Lovatt known of the existence of TOR. The Tribunal preferred Lee Lovatt's evidence on the balance of probabilities to the effect that he was aware software had installed which he had overseen with the support of the IT department. It did not accept the claimant's suggestion that Lee Lovatt was not telling the truth on the basis that the respondent was unable to produce a paper trail evidencing the authorisation. The undisputable fact is that for all the claimant's attempts at overcomplicating the evidence, two external investigations concluded the claimant had installed TOR which remained on his computer from 2014 to 2016, this fact only came to light as a result of an external audit and the claimant admitted he had installed the TOR browser.

24. On 17 March 2017 the claimant filled out an Access Review Form relating to the claimant's access to IT, which was signed by his line manager Lee Lovatt, the on-street audit manager of the Audit & Investigations department in which the claimant worked. In the section "Additional software/Network Drives Not Listed" the claimant made no mention of the software he had personally installed on the respondent's IT equipment.

<u>27 March 2018 Centrality audit exercise.</u>

25. In March 2017 the respondent changed its IT provider to Centrality who immediately conducted an audit exercise across all the employees in the business, including the claimant. On the 27 March 2018 the claimant emailed information concerning the IT listing the applications installed on his computer including a 'Start TOR browser.' Centrality were concerned and a decision was taken at board level totally unconnected with Lee Lovatt, that the matter should be investigated further by an independent IT company. There was no satisfactory evidence, apart from the claimant's say so and baseless suspicions, that Lee Lovatt had provided information relating to installations on the claimant's computer that had not been authorised by the respondent's IT department but known to Lee Lovatt in an attempt to circumvent any investigation into his own activities and knowledge. It is not credible that the

independent IT company instructed to investigate would conspire with Lee Lovatt to ensure any wrong-doing on the part of Lee Lovatt would not come to light. The investigation concerned the claimant, and it commenced as a result of the claimant installing the TOR browser in 2014 where it had remained until 2016 unbeknown to anybody within the respondent organisation, including Lee Lovatt. The claimant in his written and oral evidence, attempts at cross-examination and in submissions was preoccupied with Lee Lovett's motivation. As indicated by the Tribunal at the liability hearing, the motivation of the investigating officer was irrelevant given the particular circumstances of this case and the admissions the claimant made during the entire investigation and disciplinary process. It is notable that the claimant attempted to attribute to Lee Lovatt's investigation and the way it was handled, an intention on Lee Lovatt's part to less than objectively establish the claimant's guilt by putting words in his mouth and/or misinterpreting intentionally what was said by the claimant. This was not borne out by the contemporaneous evidence and so the Tribunal finds.

26. The respondent was concerned with the evidence that the claimant had installed the TOR browser given the position of trust the claimant held and his access to confidential information.

27. The claimant became aware that there was an issue with his computers, having received a call on 13 April 2018 from Peter Glavey employed in the IT department to the effect that something untoward had been detected on the claimant's workstation computer and his laptop was to be handed in. Without being instructed to do so the claimant immediately conducted two online anti-virus scans having attempted to unsuccessfully install anti-virus software. The claimant did not have the respondent's authority and he failed to inform anybody within the respondent of his actions.

Investigation meeting 19 April 2018

28. On the 19 April 2018 Lee Lovatt, acting in his capacity as investigator, called the claimant into a meeting without informing him of the fact that three was to be an investigation. The claimant was aware that his computers were being investigated. In contrast to the claimant's evidence, the Tribunal found this meeting should not have taken the claimant by surprise. The claimant's evidence that he as invited under a false pretence is not credible and it is notable the claimant in his written statement accepted "the initial investigation was born from a legitimate concern relating the safety of the respondent's data." He was aware there was an issue with both his desktop and laptop being investigated and should not have been surprised that questions were being asked.

29. The meeting was short; it commenced at 9.25 and concluded at 9.30 with a break of 30 minutes before being reconvened at 10.00 and concluding 10.10. Notes of the meeting were taken by a HR business partner, and record the claimant making the following admissions; the claimant had installed the TOR browser on his PC, "it bypasses restrictions to find things that, for example, Google won't be able to find" and he had used it "to find information into bailiff issues on forums for investigations I do…**I just use it as a browser**" the Tribunal's emphasis. The claimant confirmed when IT had asked him to bring in his computer, he had not installed Kaspersky "just did a scan". When asked whether there were "any other apps on your other bits of

equipment" the claimant responded, "No. no more whatsoever" explaining he had used the TOR browser "to find websites Google won't find," he was not successful "I just used it that once and that was about 12 months ago. I've not used it since." There was no suggestion by Lee Lovatt in the notes that his reference to "apps" was to smartphones and tablets and not to the claimant's computers as stated by the claimant in his oral evidence at this final hearing. The reference was clearly to computers given that was the only matter under discussion, and there was no suggestion the claimant's use of phones or tablets was ever under investigation and the claimant's suggestion that this was the case is intended to confuse and hide the reality of what was said at the first investigation meeting, and the admissions he made.

30. It is notable Lee Lovatt put to the claimant "Going back to when you installed it, given that the TOR browser has access to the deep dark web, did you not think to ask if it was ok to have installed" to which the claimant responded "It's not an illegal piece of software. Just because you have access to something doesn't mean you'll use it. We all have access to porn sites, for example, on a normal browser."

31. Lee Lovatt suspended the claimant on full pay pending a "full investigation" to be carried out by IT "as there may be a data risk here given the type of data you have access to." The claimant's response was "I feel like some type of fall guy here…there has been some sort of breach due to IT's ineptitude and they need someone to take the fall. I'd rather have the investigation carried out first before me being suspended" to which Lee Lovatt responded "the purpose of the suspension is to ensure the investigation is conducted fairly on both sides." The claimant sought an "apology from IT when its finished. I used to help people with internet security…I was intrigued at the potential of finding bailiff forums which is why I used the browsers. It was only for a couple of hours and then didn't use it again. That was about 12-months ago." It notable the claimant contradicted his earlier evidence and this fact was picked up by at disciplinary stage.

32. The claimant described himself as a computer expert in information security, criticised Lee Lovatt's lack of computer expertise and the ineffectiveness of the respondent's IT department and this was a repeated criticism throughout the disciplinary process and this liability hearing. It is notable the claimant confirmed in oral examination he had only used the TOR browser for approximately 30 minutes, and in his written statement described how he was under "extreme duress" at the time; Lee Lovatt evidence that this did not appear to have been the case at the time was preferred by the Tribunal compared to the less than credible evidence given by the claimant. The claimant's true reactions at the meeting was evidenced in the contemporaneous notes taken by HR, his criticisms of IT, its ineptitude, the and expectation of an apology from IT did not suggest the claimant was under extreme stress as alleged. Part of the claimant's case, as set in his oral and both written submissions, is his criticism of the content of the investigation notes and the fact he was not provided with a copy until much later. It is undisputed the claimant did not take any notes himself and he relies on memory, which the respondent found for very good reason was unreliable. In the claimant's written statement, he admitted inconsistent answers were given citing the reason being unable to recall a date of installation for the TOR browser "I could only recall using once before" during the "interrogation."

33. The claimant was issued a suspension letter dated 19 April 2018 that referred to the respondent's disciplinary procedures, confirming "suspension does not constitute disciplinary action and does not imply any assumption that you are guilty of misconduct…Should you wish to contact any employee who you feel would assist you…arrangements can be made for them to be available for interview." The claimant was advised "should the investigation indicate that there is an allegation you will be required to attend a disciplinary hearing." Contrary to the claimant's assertions, Lee Lovatt had not decided the claimant was guilty of gross misconduct and matter should proceed to a disciplinary beforehand "the perfect opportunity to ensure I was removed from my position." The Tribunal accepted Lee Lovatt's evidence that his task was to collate all of the evidence into a report and it was for someone else to make a decision of the disciplinary process to follow. It is clear from the evidence before the Tribunal Lee Lovatt was not the dismissing officer and he played no part in the decision to dismiss the claimant.

34. 7Elements Investigation Reports

35. The independent IT company instructed at director level to investigate was 7Elements who described itself as an "Independent information security consultancy."

36. A report was produced dated 20 April 2018 and it was evident two people had been involved in its production. One of the stated aims of the investigation was "to identify and recover evidence proving if a Marston Group employee had used a TOR browser (a pre-configurated web browser used to protect anonymity…" The approach taken was set out and evidence gathered including screenshots and exhibits taken from the laptop relevant to the investigation. The report ran to 26 pages and in the summary of findings it was confirmed the claimant had last used the TOR browser on 8 July 2016, a number of emails "were identified that show corporate data being sent to personal email accounts" and these should be investigated "to understand the level of sensitivity the document contains and if there had been a breach of confidentiality by the end user."

37. A second report was produced dated 3 May 2018 that ran to 12-pages setting out various technical information. It confirmed the claimant had "recently downloaded and executed" three anti-virus programmes on 13 April 2018 including Kaspersky. It also confirmed three movie files and one computer game had been identified suggesting "pirated copies have been saved to the asset" although no current copies of the files were found on the system. The pirated films and video game were named. In the summary it was confirmed the investigation had "revealed the presence of the 'Revo uninstaller programme and three anti-virus programmes…the user browser history prior to the use of Revo Uninstaller programme show access to cloud based solutions (Google mail and Dropbox) that are known data exfiltration routes. Access to both were concurrent with accessing internal corporate applications…it is not possible to confirm if data was exfiltrated. Installing three antivirus software products and having software which has a feature called "evidence remover" would indicate the user is knowing[ly] doing something they suspect could introduce malware and that they are using software to try and hide their activity. It should also be noted that Revo uninstaller programme has features such as browser cleaner, MS office cleaner, Windows Cleaner, Evidence Remover and an

Unrecoverable Delete function. Non- work-related software was also identified in the form of three movies and a computer game."

38. A number of emails resulted in which Savit Bowry, employed in the respondent IT department, followed up the investigations with further inquiries.

39. In an email sent to Savit Bowry by 7Elements on 10 May 2018 it was confirmed the claimant had downloaded "three executable files…that are associated with One Drive installer…it looks as he was having install issues." In a second email of the same date reference was made by 7Elements to "odd behaviours on the laptop. On the 20 February 2018 at 13.53.57 the user executed netplwiz.exe…[it] is a Microsoft programme for advanced user account management. It allows a user to change settings associated with the account and can even allow for the laptop to be accessed without a password. However, I can only state that the programme was started and whatever activity he did with the tool required elevated privileges." Evidence relating to the investigation was set out. In a third email of the same date 7Elements confirmed "I've not managed to identify the user associated with the Dropbox account. But given the tools available to remove browser history and sensitive files, I am not surprised."

<u>The second investigation meeting</u>

40. The claimant was invited to attend a second investigatory meeting on the 9 May 2018. James Thompson took notes, the claimant did not. The meeting commenced at 11am and finished 11.21 during which the claimant was asked a number of questions by Lee Lovatt. The claimant made the following admissions:

40.1 The claimant understood the TOR browser bypassed geo-restrictions and he wanted to look at forums that may be hidden by Google.

40.2 He had last used the TOR browser "about a couple of years ago…**never used it again…used it for maybe half an hour** [the Tribunal's emphasis]".

40.3 The TOR browser potentially had been used between December 2012 and 16 but the claimant could not recall using it.

40.4 The emails to which company documents had been sent were the claimant's private email addresses.

40.5 Five documents listed including spreadsheets, a sale fee memo and an investigation report into another employee was sent to the claimant's private email address on 27 January 2018. The reason given by the claimant was "because my laptop does not have One Drive installed on it. I needed to send to my private address to be able to open it on my personal laptop which could access One Drive." The claimant maintained he did not have the means to access these documents through One Drive.

40.6 The claimant was unaware of company policy that he should not install software and he installed and ran Revo on 20 February 2018 because it was a better installer that the standard Microsoft installer, it "does a much cleaner uninstall" and he had cancelled Kaspersky when he saw it was not installed.

40.7 The claimant wanted to do his own checks.

40.8 The claimant had used Dropbox on 20 February 2018 after the department stopped using it by logging onto Lee Lovatt's personal account with his permission.

40.9 "Someone" had downloaded the pirated media which the claimant transferred to a torrent file and then "probably transferred them from the pen drive to the laptop" but could not remember. The suggestion was that he had because as explained by the claimant "you wouldn't want a pen drive flashing away at you."

40.10 There was no restriction on the claimant being allowed to install software on his workstation and laptop because both were "derestricted…Most users have limited privileges, e.g. on website or what they can install or uninstall. My systems were unrestricted a while ago, the same as Lee's."

41. The claimant was not provided with a copy of the meeting notes until the Lee Lovett's investigation report to which they were annexed.

7Elements instructed to further investigation

42. Lee Lovett asked 7 Elements to conduct further investigation following the second investigation meeting in the light of the claimant's comments, and the Tribunal found the investigation fell well within the band of reasonable responses open to a reasonable employer.

43. 7Elements advised the claimant had downloaded files "associated with One Drive installer" and the dates were set out with the evidence gathered from the laptop and desk top concluding "the workstation clearly shows use of One Drive." This evidence brought into question the claimant's credibility. Reference was also made to netplwiz.exe with the relevant evidence set out. The claimant's VPN access was investigated following the claimant stating he had VPN issues on his lap. 7Elements concluded "Pete Glavey (Group engineer) confirmed that Peter Lloyd does have VPN access from his laptop and there has been no history in the time of the events of Peter Lloyd submitting a support ticket for his VPN not working." Finally, reference was also made to the Access Review Form completed and "signed by the claimant…to identify what access rights they currently have and what they should have to complete their tasks." The claimant's submission that the Access Review form was signed by Lee Lovatt is correct, but nothing hangs on this as managers were requested to sign the form after completion by the employee. There is no dispute the claimant completed the form but did not sign it as he was not required to do so.

Lee Lovett's investigation report dated 17 May 2018.

44. The report clearly cites Lee Lovett as investigator on the front sheet, with James Thompson (HR business partner who took the minutes) producing the report. This was an issue for the claimant, but not for the Tribunal who possess industrial knowledge that HR can often assist in the drafting of the report format, and it accepted Lee Lovett's oral evidence on cross-examination that the findings set out in the report were his.

45. The report ran to 19-pages to which 9 annexes were attached, including the notes taken at the claimant's investigation meetings. Under case history reference was made to the claimant, due to his role and responsibilities, "being one that grants access to highly sensitive and confidential information, including video footage of customers." This was not disputed by the claimant.

46. Lee Lovett recommended a disciplinary hearing be carried out in relation to 6 allegations "which may be deemed as misconduct or gross misconduct…" the matter was then left for David Fenwick, senior compliance business partner appointed disciplinary officer, who had no previously dealings with the claimant in respect of the disciplinary allegations.

47. The claimant was invited to a disciplinary hearing by letter dated 18 May 2018 which the claimant does not have issue with. The letter complied with the ACAS Code of Practice. The disciplinary policy and procedure together with internal investigation report dated 17 May 2018 and appendices was enclosed. The claimant therefore had sight of the investigation meeting notes prior to the disciplinary hearing.

48. Six allegations were set out:

(1) Downloading, loading or use of unauthorised and pirated software/video files on company PCs,

(2) Spending of inappropriate material to private email addresses income in contravention of the acceptable user and information security policies which may represent a disclosure of confidential information;

(3) installing software without authorisation from the IT department

(4) the use of TOR browser which has the potential to hide your Internet activity from the company when there is no requirement for you to use this;

(5) the use of Dropbox which had the potential to share company data; and

(6) the use of netplwiz.exe which has the potential to change access rights without authorisation.

49. In response to the investigation report the claimant produced a 36-page document setting out his defence and emailed to David Fenwick on 29 May at 8.33 before the disciplinary hearing. In his introduction the claimant wrote "**In the cold light of day, I've to hold my hands up and accept that on one day, my actions fell short of the company's expectations of me considering the level of access I have to confidential information**…it is my intention to vigorously defend my actions…and refute the misleading and factually incorrect evidence used in James Thompson's and the 7Elements reports…" the Tribunal's emphasis. The claimant set out his background in computing for context "an explanation for some of my actions and penchant for certain software interests" describing how he had received specialised training and provided expert advice in the use of malware diagnostic tools, and had written public tutorials to which links were provided.

50. The following points raised by the claimant are notable:

50.1 The TOR browser had been last used on 8 July 2016…apparently…installed in December 2014, but I have only James Thompson's word for that…"

50.2 "7Elements have correctly identified numerous emails that were sent form my Marston email address to my personal email addresses in the past. The recent emails form 27.1.18 consist of serval confidential documents in relation to an investigation **I personally instigated and complied the report on** before uploading the updated copy to OneDrive…"

50.3 "When I completed working on the Rossendale's investigation at home…I zipped up the entire contents and emailed them from my personal computer to my Marston email address…. this allowed me to save the zip file to OneDrive…James Thompson appears to have little appetite for discussing any of the **confidential documents** sent prior to my VPN installation…" [the Tribunal's emphasis].

50.4 "I stated at the preliminary interviews that I was unaware of the company policies surrounding the installation of unauthorised software…Lee Lovatt never suggested at any time that anyone should consult IT before downloading and installing software…" The claimant with reference to having signed receipt of the Employee Handbook which forbids the downloading of software without IT's permission wrote "I appreciate I appear to have signed a letter 3 years ago…I'd ask the panel to realistically consider that all employees in the company would have read and retained in memory every sentence of a 39-page company booklet.

50.5 The Revo uninstaller was used to uninstall software.

50.6 Kaspersky was a "proper programme which installs and that w downloaded in error…I exited the setup…and instead downloaded the applet for ESET's online scanner before running that" linking his actions to the Peter Glayey's request that he bring in the laptop for testing.

50.7 Within the body of his defence the claimant dealt with the notes taken at the investigation meeting confirming "the documents were sent to my private email address so that I could open the files with the full Microsoft word package on my own computer. **Clearly this is wrong** but that was my thinking in the moment…I'd had issues accessing One Driven my work laptop…" The claimant confirmed had attempted to "tweak the Group policy of a standard Windows account which can be accessed via the properties menu of netplwiz…" [the Tribunal's emphasis].

50.8 With reference to private emails the claimant accepted "there is a potential risk that company data could be distributed to external servers in this way (without an audit trail) …the risk is minimal but, as I accept, a risk nonetheless."

50.9 The claimant denied unlicensed software and/pirated files were found on the hard drives "period. As such, there is no risk to the business" and he believed "factually incorrect information…was designed to entrap me into incriminating myself…I have been an exemplary employee and self-employed agent…for the best part of 13 years…you have my heartfelt apologies for the trouble my

inadvertent actions have caused and I assure panel members that if I am spared the ultimate sanction of dismissal, you have my word that nothing like this will ever happen again."

The disciplinary hearing 29 May 2018

51. The claimant chose not to be accompanied and his request for the meeting to be recorded was refused by David Fenwick, a HR assistant took notes. The claimant did not take notes, and the only notes in the hearing bundle were the handwritten pages produced by the HR assistant, which the claimant was given to read after the hearing finished. There was an issue concerning whether the notes were indecipherable or not, the claimant claiming that they could not be read. The respondent produced the original notes viewed by the claimant, and there was no reason to disbelieve the claimant's evidence on this point. Fortunately, the notes were typed up later and provide to the claimant. The following was relevant:

51.1 The meeting commenced at 11am and finished at 13.10 during which six allegations were discussed, and the claimant raised questions over the ACAS Code and how the investigation personnel had been selected and by whom.

51.2 In respect of the first allegation; downloading, loading, or use of unauthorised and pirated software/video files on the company PC's David Fenwick asked the claimant if there was a business need for him to do so. When the claimant responded that the allegation was "irrelevant" David Fenwick took the view the claimant did not appreciate the seriousness of his actions.

51.3 The claimant confirmed he was unaware downloading software had to be authorised by IT, he decided what was downloaded and did not question whether he had authority or check it with the line manager stating; "it may have crossed my mind but I didn't think it was important." When asked "now that you have had time to reflect, do you feel it is important" the claimant responded "of course, wholeheartedly, I wouldn't do it now I know the company's strong position and now knowing the policies cited in the investigation."

51.4 When asked "given your role, didn't you have knowledge of the policies or that this was a breach" the claimant responded **"I had no knowledge of how serious the company treated it. On reflection I'm now aware…Before I thought it may be frowned upon but not as serious as it has been made clear**…" [the Tribunal's emphasis]. David Fenwick did not believe the claimant, given the fact he was responsible for auditing other employees for compliance, did not possess knowledge of the respondent's policies and procedures available to all on the intranet to all, including the claimant. David Fenwick genuinely believed the claimant, of all people, would have appreciated their importance and took the view that he was aware hence the comment that his actions may be frowned upon by the respondent.

51.5 The claimant denied being aware of the "specific policies that have been used here" described himself as experienced knowledge of IT and confirmed he had not thought to check with IT or line manager conceding that it would be an issue for a "normal employee" when downloading software not authorised by IT "it could get malware, infect the PC etc." He took the view that as he was

experienced “all the software I’ve downloaded is safe and not going to cause any problems…. I’m satisfied in my own abilities…I’ve been doing this since I first started with the company.” The claimant confirmed he had raised issues with IT “with such things as BWV software” and knew how to raise a ticket on the system. David Fenwick took the view the claimant could have raised all the matters included within the disciplinary allegations with the IT department, and he had intentionally not raised them with any person, including his managers.

51.6 With regards to sending confidential information to his private email addresses, this allegation was accepted by the claimant who did not think it was serious. David Fenwick disagreed, he expected someone with the claimant’s knowledge, IT experience and role that involved access to highly confidential information, to appreciate sending confidential information outside the protection given to the respondent’s IT and therefore outside its control, would be a risk to the business. It is notable the claimant in cross-examination at the liability hearing raised as an issue the lack of any stamp denoting the documents he had sent to his private email address as confidential, ignoring the fact that documents can be confidential by their very nature and he had conceded on numerous occasions that they were during the disciplinary process. David Fenwick was concerned with the claimant’s attitude towards confidential information, especially his comment that he did not think it was serious, sceptical that it had not crossed the claimant’s mind at the time given his previous IT experience and responsibility within the respondent for confidential information. David Fenwick concluded the claimant had no regard when sending confidential information from his work address to private email address and this was a serous fault.

51.7 The downloading of unauthorised software was explored. The claimant maintained the software he installed was not a risk and “had a business need” which was “not in my remit but is in my knowledge” accepting in the “cold light of day” IT should make the decision on whether software presents a risk to the business. David Fenwick was satisfied the claimant understood that software downloaded without authorisation from IT could get “malware” and the fact that Lee Lovatt had been aware the claimant downloaded iTunes and camcorder software was not mitigation. David Fenwick was aware I-Tunes was necessary for the I-Pad and surveillance software and authorised by the respondent’s IT department. David Fenwick was concerned with the claimant’s attitude in respect of downloading software, his dismissive attitude towards the IT department and his belief that he knew enough and did not require approval on the basis of his own assessment of the software. David Fenwick took the view it was unacceptable for the claimant to have clearly disregarded the seriousness of the issues in the first place, and continued in this attitude during the disciplinary process despite the risk the business could have been exposed to. He was particularly concerned that the claimant challenged him in respect of his own IT experience and concluded that the claimant felt he knew IT better than anyone else; policy, procedure and the IT department were not relevant to him despite accepting he had received a copy of the employment contract and Employee Handbook which made it clear he could not download software without permission.

51.8 With reference to the TOR browser the claimant explained he had been searching for "hidden forums, Beat the Bailiffs" and when asked how often this would happen the claimant's response was "weekly basis. I was trying to find out where Beat the Bailiffs was going next." He confirmed TOR was a place to hide and no "alarm bells went off" as it was "legal software" used "to pass Google's page ranking system. My machine is unrestricted…" David Fenwick was concerned with the claimant's responses and the fact he could use the software to hide his activity from the respondent, he was not satisfied with the explanation given and the fact the claimant did not draw a distinction between activities that he could undertake as part of his role and activities that the police undertook, the claimant having attempted to justify his use of TOR by saying the police used it to find illegal activity. David Fenwick concluded that had the claimant genuinely believed his use of the TOR browser was legitimate and for a justified work-related reason he would have discussed it with his line manager and/or the IT department. Instead, the claimant had kept the fact he used the TOR browser hidden from the respondent. The claimant accepted he had not informed the respondent.

51.9 David Fenwick was also concerned that the claimant had contradicted his evidence as to how many times he had used the TOR browser. He had said he used the TOR browser for less than one hour when he had installed it, then accepted he could have used it between 2014 and 2016. The 7Elements report confirmed the claimant had retained the browser installed onto his computer for over 18-months and as its main purpose was to hide activity, the respondent was unable to say how many times it had been used.

51.10 David Fenwick took into account the fact the claimant had not given any consideration into whether the respondent's business was at risk of hacking or data breaches given its involvement in government contracts and court enforcement for the MOJ. He was greatly concerned with the claimant's attitude towards security, and his preoccupation at the disciplinary hearing with a lack of motivation and a failure on his part to understand or appreciate the seriousness of his actions.

51.11 It is notable the minutes reflect the claimant's response when asked whether Lee Lovatt was aware the claimant had installed TOR. The claimant's response was "I'm not sure, probably not…but Lee knew my background in IT security…helping out on forums for decades…pass on advice and training" confirming he was "computer savvy" When asked if he had found any forums using TOR the claimant stated he had not and "must have used it for less than an hour." The reality is that the claimant was sure Lee Lovatt was unaware of the TOR browser because he had not informed him, or indeed anybody within the respondent, of its existence.

51.12 The claimant maintained he had not "fully checked" the contract and had "dug" the Handbook "out of the cupboard last week." Training was discussed which the claimant was unable to recall, and he confirmed software had not been brought up at team meetings, the claimant's colleagues being "less than novice" and no experts on computers. David Fenwick was concerned with the claimant's attitude and he did not accept his lack of knowledge had any basis,

concluding the claimant had demonstrated to him the respondent's documentation, including the contract, were unworthy of his time and attention.

51.13 The claimant denied using Dropbox and confirmed he had used Netplwiz when attempting to reinstall OneDrive, which "on reflection" he should have referred to IT but "at the time and given my experience I didn't think I had to…I used Revo to uninstall…used and known by IT professionals." David Fenwick was concerned that when the claimant had experienced a serious issue such as corruption of One Drive, his response had been to attempt a reinstall and not refer it to IT. David Fenwick concluded the claimant had demonstrated to him throughout the hearing by his overall demeanour and responses to the questions raised, that he did not appreciate the seriousness of his actions and the risk the respondent had been exposed to as a result of them.

52. David Fenwick gave the claimant a full opportunity to put forward his defence to the six allegations raised and dealt with individually. The claimant at the liability hearing put to David Fenwick in cross-examination that he had not read the written defence beforehand, which was denied. It is clear from reading the notes of the meeting that the claimant, over a period of some 2 hours and 10 minutes provided evidence in relation to each allegation; he did not check to see if David Fenwick had read the defence and it was open to him to clarify or elaborate on any aspect of it, which the claimant did. He also questioned procedural matters, such as what policy prevented the respondent from recording the hearing, and what would happen to the notes afterwards. The claimant did not ask whether a representative from 7Elements could appear at the hearing in order to be cross-examined on the contents, a matter he raised as a criticism of the process at the liability hearing. David Fenwick relied on the 7Elelements investigation, he reasonably understood that independent IT experts had investigated matters the claimant subsequently conceded he had carried out, and was entitled to take this into account.

53. The disciplinary hearing and process before and after the hearing, was carried out in accordance with the ACAS Code of Practice and fell well within the range of reasonable responses open to a reasonable employer.

54. Having considered all of the evidence, including the independent expert evidence on which David Fenwick was entitled to rely, the admissions and contradictions in the claimant's evidence, including the written defence, he concluded five of the six allegations were proven, the unproven allegation being the use of Dropbox. He held a genuine belief, given the evidence, that the claimant had transferred pirated videos/game and watched/played them on his company laptop due to not wanting to see a flashing light on his memory stick. He concluded the claimant's actions had the potential to bring the respondent into disrepute.

55. David Fenwick took the view that the claimant's actions in respect of sending confidential material to his personal email addresses seriously breached the implied term of trust and confidence and the claimant should have known the information was confidential i.e. a sale and disposal sheet had been included, and it was incomprehensible that the claimant had acted in this way, especially given his role in the business, the high level of confidential information he had access to when auditing, investigating, enforcement and dealing with compliance. The claimant had admitted installing the TOR browser and Revo uninstaller that had the potential to

remove any history of software installation, and David Fenwick was "extremely concerned" the claimant had a facility, hidden from the respondent, that enabled him to search the dark web and this was a significant risk to the business. David Fenwick held a genuine belief despite the claimant's denials that he had not used the TOR browser for anything other than a business need, that the claimant had no legitimate business need, he had contradicted his evidence, his conduct was both a serious breach of the IT system and "significantly impacted upon the trust and confidence the respondent held in the claimant".

56. In oral evidence David Fenwick confirmed that either one of the allegations of gross misconduct found against the claimant would have resulted in his dismissal. He held a genuine belief that cumulatively the claimant's behaviour amounted to a serious breach of confidentiality and the respondent's security, with the potential to bring the respondent into disrepute and the implied contractual term of trust and confidence had been broken irretrievably. He took a view which fell well within the band of reasonable responses open to a reasonable employer, that even if the claimant had not read the policies and procedures or the terms set out in his employment contract, his actions were such that no reasonable person would have thought it was acceptable to do what the claimant did.

57. On the issue of mitigation, David Fenwick took into account the written defence and decided its contents did not mitigate the seriousness of the claimant's actions. David Fenwick concluded the claimant had little understanding of the potential impact and this did not change during the disciplinary process. The claimant's clean disciplinary record and length of service was not sufficient mitigation given the breakdown in trust and confidence resulting from the claimant's misconduct, and his lack of appreciation in terms of the seriousness of his actions. In short, David Fenwick did not accept the claimant's explanations for his actions had any basis to it, and the Tribunal took the view, on the balance of probabilities, that he did not need another medical report to come to this view.

Dismissal 7 June 2018

58. In a letter dated 7 June 2018 the claimant was dismissed without notice. Reference was made to the individual allegations and David Fenwick's decision-making process that included considering the claimant's admissions. Reference was also made to the policies and procedures, and the claimant's "duty to familiarise yourself with all the policies and procedures and indeed acknowledged during the disciplinary hearing that you were 'most likely aware' that policies and procedures relevant to your role were included on the intranet and when asked if you ever felt the need to read them, you responded by stating that you 'never felt an intrinsic need to read them" and "a lot of people probably don't read them.' Such comments are considered unworthy mitigation for your own shortcomings. Furthermore, even if you hadn't read the policies and procedures, your activity is such that no reasonable person would have thought it acceptable to do what you have done."

59. Reference was made by David Fenwick to the claimant's written defence as follows: "Both your written defence and your explanations at the disciplinary hearing were not considered relevant mitigation to justify your actions and do not remove the fact that the original allegations have been proven…the nature of the software downloaded also causes considerable concern i.e. TOR Browser and Revo

uninstaller…there was an explicit opportunity for you to confirm additional software downloads on the Access Review form which you confirmed you completed in March 2017…you consciously omitted these…because you didn't know company policy regarding software."

Appeal

60. The claimant appealed on 12 June 2018 in a 5-page document criticising the investigation and the disciplinary hearing, maintaining there existed a lack of reasonable belief, alleging David Fenwick "simply doesn't understand IT…he didn't consult an IT professional…in relation to the counter-evidence I suggested." The claimant also explained "**when I did admit to sending a document that contained confidential information that Id compiled, I had a perfectly reasonable and legitimate purpose for so doing, namely…covering an unethical and highly illegal director driven profiteering policy**" [the Tribunal's emphasis]. The claimant alleged that he had not been provided all the evidence cited in the investigation in breach of the ACAS Code as some of the evidence was "copied and pasted" from an email received by 7Elements. This was one of the matters explored by the claimant during the liability hearing and it transpired the documents were identical and the claimant had been provided with all the evidence relied upon.

Grievance

61. On the 12 June 2018 the claimant raised a grievance that ran to 4-pages which included a number of matters ranging from criticisms of the investigation to David Fenwick failing to postpone the disciplinary hearing to a later date "to allow himself time to read, digest and fact check my counter-evidence submitted the previous week. He admitted that he hadn't had time to read the 36-page defence document prior to starting the disciplinary hearing…which is highly unfair…this denied me the opportunity to question vital parts of false evidence…his dismissal letter shows he paid little attention to anything I wrote in my defence." With reference to these specific complaints the Tribunal notes the claimant was given opportunity at the disciplinary hearing to put forward his defence and question "vital parts of the evidence" and his written defence was taken into account by David Fenwick, who relied upon the claimant's admissions and the 7Elements expert report, which he was entitled to do.

62. The claimant followed the grievance letter up with a further letter dated 28 June 2018 in which he alleged the investigation had been used against the claimant "to ensure the trumped-up evidence and conclusions resulted in my dismissal" to save money and reduce the headcount.

63. In the letter inviting the claimant to the appeal hearing he was informed recordings of meetings was not allowed, but notes would be taken and provided. The invite letter complied with the ACAS Code of Practice.

The appeal hearing

64. The appeal hearing took place at 14.08 on 2 July 20118, Deborah Cooper acted as chair supported by Carol Imreie, head of group HR operations, and a HR assistant as note taker. The claimant chose not to be accompanied on the basis that

"nobody knows the case better than me." He was given the opportunity to fully explore and explain his arguments, including linking the dismissal to a reduced headcount.

65. At the hearing the claimant, in answer to one of his appeal points, was informed by Carol Imreie she had been notified of the presence of the TOR browser on the claimant's laptop by Centrality during an audit of the entire business, and she authorised the investigation and started the process.

66. Deborah Cooper did not accept the claimant, who she believed was an expert at his job and exemplary employee, was dismissed due to changes made to the audit department as asserted by the claimant. The claimant was invited to give an explanation "in layman's terms" and Deborah Cooper considered a number of allegations raised against Lee Lovatt who had allegedly according to the claimant "trumped up" the charges, which she dismissed given the undisputed fact that an independent report had been obtained following a request from Carol Imrie and there was no connection with Lee Lovatt.

67. A key matter for Deborah Cooper was the claimant's attitude towards the TOR browser and the fact he did not appear to understand that he had admitted downloading a browser that hide his activity from the respondent, and even at appeal stage did not see an issue with this, despite an awareness of its suspicious nature. Deborah Cooper came to a view that the only possible explanation for the claimant's behaviour and the fact he had kept it hidden from the respondent, was he knew he should not have been using the TOR browser, and it did not need a policy, a procedure or training to inform him of this. There was a concern within the respondent as it could not be one hundred percent certain what the claimant had used the browser for because the searched he had carried out were hidden, and when this was put to the claimant Deborah Cooper was "shocked" by his response when he argued TOR was no different to Google Chrome, when it clearly was.

68. Deborah Cooper explored fully the claimant's arguments and responses, including his admission that he knew of the respondent's policies regarding IT use existed, but not the specifics. It is notable in cross-examination of Lee Lovatt the claimant suggested he did not know of the policies, in direct contradiction of the evidence he gave at appeal and this raised further questions over his credibility. It is notable the claimant at the end of the appeal hearing confirmed he had a fair hearing and been listened to, which was not disputed by the claimant at this liability hearing.

69. The Tribunal was satisfied Deborah Cooper had considered all of the claimant's written and oral evidence before she made her decision, and having reflected on it and the fact the claimant had worked for the respondent for 3-years and had access to highly confidential information, she relied upon the 7Elements expert report in which a number of significant concerns were raised. Deborah Cooper was concerned with the attitude the claimant had shown during the disciplinary process towards the seriousness of the allegations, especially the TOR browser and confidentiality, the fact he had indicated his awareness of the respondent's policies but had not bothered to read them and the disregard he had for the respondent's IT experts and their authority. It is notable the attitude exhibited by the claimant during the disciplinary and appeal hearings was duplicated at this liability hearing; the claimant clearly considered his expertise in IT allowed him to

take decisions that would not ordinarily be taken by other employees of the company.

70. Deborah Cooper concluded that either individually or cumulative the five allegations had been made out and constituted gross misconduct and the appeal was not upheld.

Dismissal of the appeal

71. The claimant's appeal was dismissed by a letter dated 17 July 2018 in which reference was made to the various grounds relied upon by the claimant, including the fact that "given your role as an on-street audit & investigations officer, a position that you have held for 3-years, and your access to confidential information in the business, the decision was made at board level to sanction a forensic examination of your system by a specialised IT company." The evidence provided by 7Elements was referred to and in relation to the TOR browser Deborah Cooper concluded "…your activities were a real concern for the business given your access to all the company operating systems."

72. Deborah Cooper confirmed she had spoken with David Fenwick and she was satisfied he had taken the claimant's written defence into account and "his position, with which I agree, is that the reasons you put forward or using the systems for the purpose you detailed do not justify your actions." Deborah Cooper referred to the claimant's employment record but given there was a "clear breach of trust" the dismissal was upheld. Turning to the individual allegations Deborah Cooper found:

72.1 With reference to the unauthorised use of pirated software/video files that the claimant's defence was not focused on the illegality of his actions but the fact he played the "pirated files from a pen drive rather than downloading directly on to your laptop." She concluded; "I fail to see the difference; the playing of pirated material on a company laptop is not acceptable and is a breach of our policies and procedures. "

72.2 With reference to sending commercially sensitive material to a private email address Deborah Cooper noted the claimant had accepted it was wrong, and "your inference that the compiling of this report is the reason for your termination is simply not true. The investigation was sanctioned by the business and the production of the report part of your job…"

72.3 With reference to installing software without authority and the TOR browser Deborah Cooper dealt with the claimant's claims that he was unaware and his manager had never indicated that this was not permitted, confirming her view that ignorance was no defence "part of your job was to ensure that the front-line enforcement staff were complying with company operational guidelines, yet you claim not to have knowledge of company policy…you agreed that you were guilty of doing the wrong thing but for the right reasons, that if you had thought about the consequences of your behaviour then you would not have done it. It is on this point where your defence and the view of the disciplinary manager differ…there can be no legitimate reason for you to have the software on your system…it is clear that the software is neither essential nor beneficial to you doing your job. It is unauthorised and was never declared…"

72.4 Deborah Cooper dealt with netplwiz as follows: "what you failed to accept is the premise that you did not have the authorisation to fix any IT issues or uninstall One Drive…"

72.5 Deborah Cooper informed the claimant that his allegation of reducing the head count and cost saving by dismissing him and another colleague was refuted and he was being replaced. The undisputed evidence before the Tribunal at the liability hearing was that he had been replaced and there was no evidence whatsoever that the claimant was dismissed to avoid a redundancy/notice payment as suggested by the claimant during these proceedings. Deborah Cooper rejected the claimant's argument that he had been dismissed as a whistleblower into director/management level corruption when "the investigation you were involved in was sanctioned by the business to uncover and report any poor practices."

72.6 The claimant's grievance was also dealt with and dismissed.

73. The Tribunal found the appeal hearing complied with the ACAS Code of Practice. Deborah Cooper was independent, she reviewed all the relevant documentation including the 7Elements investigations, the contractual documents, policies and procedures and the claimant's written defence, appeal and grievance. Deborah Cooper held a genuine belief based upon a reasonable investigation that the claimant had been provided with all the relevant evidence, he had the opportunity to put forward his grounds of defence fully and respond to all the allegations.

74. The effective date of termination was 7 June 2018.

Law

75. Section 94(1) of the Employment Rights Act 1996 ("the 1996 Act") provides that an employee has the right not to be unfairly dismissed by her employer. Section 98(1) of the 1996 Act provides that in determining whether the dismissal is fair or unfair, it is for the employer to show the reasons for the dismissal, and that it is a reason falling within section 98 (2) of the 1996 Act. Section 98(2) includes conduct of the employee as being a potentially fair reason for dismissal.

76. Section 98(4) provides that where the employer has fulfilled the requirements of subsection (1), the determination of the question whether the dismissal if fair or unfair (having regard to the reasons shown by the employer) depends on whether in the circumstances (including the size and administrative resources of the respondent's undertaking) the employer acted unreasonable or reasonably in treating it as a sufficient reason, and this shall be determined in accordance with equity and the substantial merits of the case.

77. Where the reason for dismissal is based upon the employee's conduct, the employer must show that this conduct was the reason for dismissal. For a dismissal to be procedurally fair in a case where the alleged reason for dismissal is misconduct, Lord Bridge in Polkey –v- A E Dayton Services Limited [1981] ICR (142) HL said that the procedural steps necessary in the great majority of cases of misconduct is a full investigation of the conduct and a fair hearing to hear what the employee has to say in explanation or mitigation. It is the employer who must show

that misconduct was the reason for the dismissal, and must establish a genuine belief based upon reasonable grounds after a reasonable investigation that the employee was guilty of misconduct – British Home Stores Ltd v Birchell [1980] CA affirmed in Post Office v Foley [2000] ICR 1283 and J Sainsbury v Hitt [2003] C111. In short, the Tribunal is required to conduct an objective assessment of the entire dismissal process, including the investigation, without substituting itself for the employer.

78. The ACAS Guide, 'Discipline and grievances at work' states that, when deciding whether a disciplinary penalty is appropriate and what form it should take, consideration should be given to, among other things, the employee's disciplinary record (including current warnings), general work record, work experience, position and length of service; any special circumstances that might make it appropriate to adjust the severity of the penalty; and whether the proposed penalty is reasonable in view of all the circumstances. The evidence before the Tribunal was that the respondent had complied with the Guide.

79. The Court of Appeal in British Leyland (UK) Ltd v Swift [1981] IRLR 91 set out the correct approach: "If no reasonable employer would have dismissed him then the dismissal was fair. But is a reasonable employer might reasonably have dismissed him, then the dismissal was fair…in all these cases there is a band of reasonableness, within which one employer might reasonably take one view and another reasonably take a different view.

80. In between extreme cases of misconduct there will be cases where there is room for reasonable disagreement amongst reasonable employers as to whether dismissal for the misconduct is a reasonable or unreasonable response: LJ Mummery in HSBC Bank Plc v Madden [2000] ICT 1283.

81. The question for the Tribunal is the reasonableness of the decision to dismiss in the circumstances of the case, having regard to equity and the substantial merits of the case. The Tribunal will not substitute its own view for that of the respondent. In order for the dismissal to be fair, all that is required is that it falls within the band of reasonable responses open to employer. It is necessary to apply the objective standards of the reasonable employer – the "band of reasonable responses" test – to all aspects of the question of whether the employee had been fairly dismissed, including whether the dismissal of an employee was reasonable in all the circumstances of the case.

82. The test remains whether the dismissal was within the range of reasonable responses and whether a fair procedure was followed. Section 98 (4) provides that where the employer has fulfilled the requirements of subsection (1), the determination of the question whether the dismissal if fair or unfair (having regard to the reasons shown by the employer) depends on whether in the circumstances (including the size and administrative resources of the respondent's undertaking) the employer acted unreasonable or reasonably in treating it as a sufficient reason, and this shall be determined in accordance with equity and the substantial merits of the case.

Conclusion: applying the law to the facts

83. In his written submissions the claimant has referred to a number of cases. He relies on Gogay v Herefordshire County Council [2000] IRLR 703 CA and Agoreyo v London Borough of Lambeth [2017] EWCH 2019 HC arguing that the suspension was a breach of the implied term of mutual trust and confidence and not a neutral act. The claimant did not resign when he was suspended on full pay, and the letter of suspension made it clear it was a neutral act. It is notable in oral evidence on cross-examination that claimant conceded it was not part of his pleaded case and he accepted Lee Lovatt could suspend on the basis of evidence of a potential data breach. The Tribunal found there was no merit in the claimant's arguments.

84. The Tribunal was also referred to Salford Royal NHS Foundation Trust v Roldan [2010] IRLR 721 and Miller v William Hill Organisation Ltd EAT 0336/12 by the claimant. In Miller the EAT acknowledged that there is a limit to the steps an employer should be expected to take to investigate an employee's alleged misconduct. It will depend on the circumstances of the case, including the amount of time involved, the expense and the consequences for the employee of being dismissed. The EAT considered that it would not have been too onerous for the employer to watch five hours of CCTV footage which would have supported M's version of events and not involved any additional expense and the only conclusion the tribunal could have reached was that the investigation which had been carried out prior to the decision to dismiss M for theft was not as thorough as the circumstances warranted. It therefore substituted a finding that M had been unfairly dismissed. Mr Lloyd's case can be differentiated from that of Ms Miller; he had admitted to a number of the allegations put to him, not least installing and using the TOR browser and transferring confidential documents to his own email address. The respondent had commissioned an expert IT report, asked 7Elemets a number of questions which they answered in clarifying emails and there was no requirement for the respondent to go to the time and expense of sending 7Elements or another IT expert the grounds of the claimant's defence. In short, David Fenwick and Deborah Cooper did not believe the claimant, he had contradicted himself, for example, about how much he had used the TOR browser (as he had also contradicted himself at this liability hearing) and as far as they were concerned the mitigation put forward for using the TOR browser and transferring confidential information, both acts admitted by the claimant, was not accepted as an explanation.

85. The Tribunal does not intend to repeat its findings above, in short, it accepted Lee Lovatt and Deborah Cooper held a genuine and reasonably held belief that the claimant was guilty with insufficient mitigation (other than his clear and excellent employment record) which did not outweigh the claimant's actions whether he had been given training and/or read the respondent's policies and procedures or not. The ACAS Guide emphasises that the more serious the allegations against the employee, the more thorough the investigation conducted by the employer ought to be. I the claimant's case there had been an investigation that fell well within the band of reasonable responses, David Fenwick and Deborah Cooper's assessment was that the explanations provided by the claimant did not provide a plausible reason for his admitted actions. David Fenwick and Deborah Cooper did not accept, having considered the claimant's evidence and arguments, that Lee Lovatt had falsified,

misrepresented and filtered evidence. The Tribunal agreed; there was no satisfactory evidence Lee Lovatt acted as alleged by the claimant, he did not compile to 7Elements report and had no hand in its commission or the evidence 7elements considered. David Fenwick and Deborah Cooper were entitled to rely on the independent IT expert report and take a view on the claimant's explanation for his actions, and conclude they did not believe him.

86. The claimant also referred to Brito-Babapulle v Ealing Hospital NHS Trust [2013] IRLR 854, EAT, in which the EAT noted that the Tribunal's approach gave no scope for consideration of whether mitigating factors rendered the dismissal unfair, notwithstanding the gross misconduct. Such factors might include the employee's long service, the consequences of dismissal and any previous unblemished record. The Tribunal was suggesting that the existence of gross misconduct — which is often a contractual issue — is determinative of whether a dismissal is unfair, whereas the test for unfair dismissal depends on the separate consideration called for under S.98 ERA. Mr Lloyd submitted that the respondent had ignored the mitigating factors "surrounding their complete failure to supply me with (a) the relevant IT policies…and (b) complete lack of training. The Tribunal did not agree with the claimant. The respondent did take these factors into account, concluding the claimant could be criticised for failing to read the policies that were on the intranet, of which he was aware and gave conflicting evidence on this point, and he did not need training to inform him that downloading and using a TOR browser was an act of gross misconduct as was transferring confidential company information to his own email address. David Fenwick and Deborah Cooper, having considered all the claimant had to say (including his written documents) came to a genuine belief the claimant, who was experienced in IT matters and believed himself to be above the reach of the respondent's IT department, should have known better than to keep the installation and use of the TOR browser hidden and his contradictory evidence on when and how many times he had surfed the deep dark net caused them concerns as there was no way of knowing what the claimant had been up to due to the very nature of the TOR browser which hid the searches carried out. The evidence before the Tribunal was Deborah Cooper took the reasonable and justified view this allegation alone was sufficient to dismiss the claimant; and his attitude towards the seriousness of his actions exhibited at the appeal hearing caused her to doubt his understanding and it brought into questions the arguments he raised in mitigation, including his veiled allegations of whistleblowing and the dismissal being a cloak for redundancy.

87. It is notable in East of England Ambulance Service NHS Trust v Sanders EAT 0319/15 the EAT emphasised Brito-Babapulle is not authority for the proposition that Tribunals must look at mitigating factors not identified by the claimant. The Tribunal in the case of Mr Lloyd noted the EAT's relevant observation that dismissal for gross misconduct will usually be fair (whatever the circumstances) but that in a 'small number of cases', the mitigating factors could be such that no reasonable employer would have dismissed. On the balance of probabilities and taking into account the fact that the Tribunal should not substitute its own view for that of the respondent, it found dismissal for gross misconduct was not unfair in the light of the claimant's mitigation given the position he held including the access to confidential information, his attitude during the disciplinary process, the intentional failure to read the respondent's policies and procedures and comply with the terms of his employment contract.

88. MacKie v Awe Plc ET/2701393/2014 a first instance decision is relied upon by the claimant. The facts of the case can be differentiated from those in Mr Lloyd' case. The claimant submitted that one of the confidential memos he forwarded to his own email address had already been sent via an "unsecure" email to approximately one-hundred self-employed contractors by the respondent and therefore the dismissal was unfair. The claimant's case can be differentiated on the basis that he sent the confidential information to his personal email address without the respondent's knowledge and without the respondent being assured its data security and confidentiality was secured, and it was not at risk of being hacked. In contrast, the respondent risk assessed the emails sent to self-employed colleagues who were bound by policies, procedures, confidentiality and data protection as the claimant was and had been when he worked on a self-employed basis and the respondent had risk assessed the use of any email address provided.

89. Turning briefly to the agreed issues, with reference to the first and second issue, namely, the Tribunal found misconduct is potentially a fair reason for dismissal under S.98(2) ERA, and it was reasonable for the respondent to treat that reason as a sufficient reason to dismiss in the circumstances under S.98(4) ERA. The central issue in this case was whether the decision to dismiss fell within the band of reasonable responses. It is a well-known principle set out in case law that in some cases there is a band of reasonableness, within which one employer might reasonably take one view and another reasonably take a different view. The Tribunal concluded that in Mr Lloyd's case, given his admissions, especially those in relation to the TOR browser and transferring confidential company documents to his own email account and the unsatisfactory explanation provided for his actions, specifically with reference to the serious matter of the TOR browser, the decision to dismiss fell well within the band of reasonable responses open to a reasonable employer. The Tribunal has further elaborated on its findings as set out below when dealing with issue number five.

90. With reference to the first and second issue, namely, did the Respondent act reasonably in the circumstances (having regard to the size and administrative resources of the Respondent) and in accordance with equity and the substantial merits of the case, in treating conduct as a sufficient reason for dismissing the Claimant (s98(4) Employment Rights Act 1996), the Tribunal found that it did for the reasons set out above. The claimant's submissions to the effect that he as somehow prejudiced from not receiving any notice of the first investigation hearing, not being asked to sign meeting notes, alleged filtering of evidence relating to the OneDrive reinstall, alleged derestriction on his IT equipment, were a defection from the real issues in the case, namely his admitted guilt in relation to the TOR browser, pirated material and confidential documents which he admitted was "an error of judgement on my part" during oral submissions.

91. With reference to the second issue, namely, did the Respondent hold a genuine belief in the claimant's misconduct, the Tribunal found that it did. It had sufficient evidence before it, not least the contents of the 7Elements investigations and the claimant's admissions that he had used authorised pirated software/video files on company PCs; sent confidential material to his private email addresses in contravention of policy; installed software without IT authorisation; used the TOR browser which has the potential to hide internet activity from the company in the absence of a requirement to do so and used netplwiz.exe which has the potential to

change access rights without authorisation. As set out in the findings of facts above, the Claimant's assertion to the effect that David Fenwick did not hold a genuine belief in his guilt was not supported by the evidence. On the balance of probabilities, the Tribunal finds David Fenwick did not fail to consider all the available evidence including the claimant's s written defence document, which the Tribunal found was not ignored the outcome letter having expressly referenced the written defence. The claimant's basis for his argument that David Fenwick "ignored" his defence partly lies in the fact that the claimant's offer to adjourn the disciplinary hearing to another date was rejected and the hearing went ahead. The claimant, who was given the option of exploring his defence in full in relation to each and every allegation at the disciplinary hearing, did so with the result that one of the grounds was found in his favour. The claimant attempted to downplay this fact at the liability hearing, which does not go to his credit.

92. In short, it was open to David Fenwick and Deborah Cooper to question the claimant's explanations; for example, neither believed the claimant was not aware the TOR browser could not be installed and took the view that the fact the claimant had kept his use of the TOR browser hidden from 2014 to 2016 reflected the true position. He knew very well it was not allowed and did not require a policy, procedure or training to inform him of this. The claimant in oral submissions argued the charges were "trumped up" which was clearly not the case given the 7Elements report, the claimant's admissions and his unsuccessful attempts at explaining his behaviour that included trying to blame his line manager, Mr Lovatt, who was totally oblivious to its existence. The claimant submitted the counter-evidence had not verified. Given the fact the conduct was admitted David Fenwick and Deborah Cooper, who had considered the expert investigation carried out by two IT companies and Lee Lovatt's investigation pulling all the evidence together, did not require yet more expert evidence to determine whether they accepted the claimant's explanation or not. Both were entitled to base their decision on the facts as admitted by the claimant at the time and reach a judgement on his explanation for the gross misconduct. The Tribunal recognises that there are cases where it would be unreasonable for an employer not to investigate the employee's explanation for it, but not in the case of Mr Lloyd. David Fenwick and Deborah Cooper were fully aware of the policies and procedures on the intranet, the contractual terms to which the claimant was bound and the expert evidence, acting within the range of reasonable responses when they considered all of the evidence, as related above in the findings of facts. In the light of the claimant's admissions, the explanations put forward and mitigation, it did not fall outside the band of reasonable responses for the respondent to disbelieve the claimant and reach the conclusion it did.

93. Turning to one matter the claimant relied upon as mitigation in his submissions, namely, "other employees found guilty of similar actions in the company" the claimant did not raise any examples of other employees committing similar acts, and he did not put to the respondent's witnesses the proposition that other employees had downloaded and used a TOR browser for the obvious reason that the claimant was the only person who had committed this act of gross misconduct.

94. With reference to the third issue, namely, did the Respondent have reasonable grounds for its belief that the Claimant behaved as alleged, the Tribunal found that it did. David Fenwick and Deborah Cooper were entitled to rely upon the

independent expert evidence gathered from two IT companies, one company having been instructed to investigate at board level. The claimant's assertion that the Respondent did not have reasonable grounds for its belief, because he did not receive training in the applicable IT policies and procedures by Lee Lovatt, David Fenwick and the Head of Department, had no basis for the reasons already stated.

95. With reference to the fourth issue, namely, did the Respondent conduct a reasonable investigation into the claimant's misconduct, the Tribunal found it did and David Fenwick was entitled to rely upon the independent expert evidence provided by 7Elements and Lee Lovett's report. The Claimant's assertion Lee Lovett had conducted a limited and ineffective had no basis. He had not filtered the evidence, falsified the evidence or misrepresented the evidence in the Investigation Report.

96. With reference to the fifth issue, namely did the decision to dismiss fall within the band of reasonable responses open to a reasonable employer in the circumstances, the Tribunal found it fell well within the band of reasonable responses taking the allegations found against the claimant singularly or cumulatively. Lee Lovatt was entitled to accept the 7Elements reports as true in the investigation and David Fenwick in the disciplinary hearing, bearing in mind the claimant's admissions as entitled to rely upon it. Neither David Fenwick or Deborah Cooper accepted the claimant's explanations set out in the written defence (counter-evidence) which disputed the accuracy of the 7Elements report and the conclusions drawn. They were entitled to reach this conclusion having considered and rejected what the claimant said, even if the claimant believed he was the more expert in IT matters than they or Lee Lovatt were. There was no satisfactory evidence had been falsified, filtered or misrepresented evidence.

97. With reference to the sixth issue, namely, has the Respondent followed a fair procedure, the Tribunal found that it had. It was not an unfairness to invite the claimant to an investigation meeting on 19th April 2018 without notice and nor was there any requirement to advice the claimant he could be accompanied at the investigation meeting on 19th April 2018 as per the respondent's policy. Prior to the meeting on 19 April 2019. It is notable the claimant never asked to be accompanied at the disciplinary and appeal hearing, despite being informed that this was his tight and the Tribunal finds the claimant's argument that he was not informed of a non-existing right to be accompanied at the investigation meeting a spurious attempt to build up a case which has no legal or factual basis.

98. The claimant was not advised he could be accompanied to the investigation meeting on 9th May 2018, the respondent's Policy did not provide for this. In any event, there is no requirement under the ACAS Code of Practice for an employee to be accompanied at an investigation meeting. The claimant was asked to read over the meeting notes of 9th May 2018 following the meeting; he was unable to decipher the writing and therefore signed the first page only. The claimant provided written comments on the aspects of the meeting notes with which he disagreed. It is notable the claimant took no notes at the time. It was not unfairness for the claimant not to sign the meeting notes of 9th May 2018 to confirm their truth.

99. As indicated above, the claimant was aware an investigation was taking place, he had been requested to hand in his laptop and Lee Lovall made it clear at the first investigation meeting which ran for 5 minutes questions were being asked

about this. There was no requirement to inform the claimant prior to the meeting taking place and nor was it an unfairness for the claimant not to be told who instigated the investigation, information subsequently provided to the claimant during the disciplinary process when he was informed the decision had been made at director level and at the appeal hearing the name of the director was provided. If there was any unfairness, this was put right at appeal in any event.

100. The claimant was not provided with the meeting notes of 19th April 2018 immediately following the meeting and he was not asked to sign the meeting notes of 19th April 2018 to confirm their truth, but this did not amount to an unfairness. The claimant was provided with a copy of the 19 April 2018 meeting notes in the investigation pack prepared by Lee Lovatt, on which he commented prior to the appeal hearing taking place, as indeed he also amended and commented on the disciplinary hearing notes before the appeal hearing.

101. The Tribunal preferred David Fenwick's evidence to the claimant's suspicions that he had failed to read the written defence prior to the disciplinary hearing; and it did not accept the claimant's unsubstantiated submission that the contents of the written defence in the disciplinary hearing had not been addressed. The claimant could put forward his defence fully and clearly in the disciplinary meeting and David Fenwick had not failed to establish the essential facts prior to his decision to dismiss the claimant. He had considered the claimant's clean 3-year employment record, and did not accept the claimant's explanation that the respondent had failed to provide him with the IT policies and training in relation to those policies (Acceptable Use, Information Security Brochure). David Fenwick reached a genuine belief based on the evidence before him that the claimant was aware of the existence of the policies on the intranet and chose not to read them. He did not need training or a policy to inform him that downloading the TOR browser without authority or informing anybody within the respondent when using it from 2014 to 2016 (the claimant's evidence on how much he used it was conflicting) under the respondent's radar, could amount to an act of gross misconduct resulting in his dismissal.

102. The claimant's motives were addressed and discounted. It is clearly recorded in the appeal meeting minutes that motive was addressed and the claimant's explanations rejected. Deborah Cooper had not failed to address all relevant points of appeal in the appeal hearing, for example, she had spoken with David Fenwick and was satisfied he had considered the claimant's written defence and did not accept any lack of training as mitigation. The claimant's grievance was also considered and the Tribunal did not find the respondent had breached the ACAS Code of Practice in any way.

103. With reference to the seventh issue, namely, remedy, as the claimant was unsuccessful in his claim there is no requirement for the Tribunal to consider this. The parties were invited to make submissions on contribution, and had the claimant been successful the Tribunal would have gone on to find it was just and equitable to reduce any basic and compensatory award (s.123 Employment Rights Act 1996 by 100 percent given its findings above. The claimant was both culpable and blameworthy for his actions and the Tribunal did not accept he had no knowledge that his conduct was wrong, accepting the respondent's evidence that the claimant given the position he held, did not need a policy, procedure or training to know that downloading and using a TOR browser was wrong.

104. Had the Tribunal accepted the claimant's evidence that he did not possess the requisite knowledge (despite the contradictions in that evidence) it would have gone on to find the claimant was culpable and blameworthy on the basis that he intentionally did not access and read the respondent's policies and procedures and skim read the terms of his contract and then used his failure as a shield to allegations of gross misconduct.

105. In conclusion, the claimant was not unfairly dismissed, his claim for unfair dismissal is not well-founded and is dismissed.

23.8.19

_____

Employment Judge Shotter

JUDGEMENT & REASONS SENT TO THE PARTIES ON

17 September 2019

FOR THE SECRETARY OF THE TRIBUNALS