Internal Audit
Finance and Customer Services

Theft of 21 Laptops from Norfolk House, Rotherham: 26th October 2011 – Review of the Council's Response.

Final Report.

Internal Audit - Finance and Customer Services

Theft of 21 Laptops from Norfolk House, Rotherham: 26th October 2011 - Review of the Council's Response

Finance and Customer Services

Theft of 21 Laptops from Norfolk House, Rotherham: 26 October 2011 - Review of the Council's response

1 Objectives of this report

1.1 This report follows an audit of details held by the Council relating to the theft of 21 Laptops from Norfolk House, Rotherham, on 26th October 2011, enquiries made regarding the theft and actions taken by the Council. It has been produced in response to a request on 25th September 2015 from the Leader of the Council (Councillor Chris Read) and Commissioner Stella Manzie, former Managing Director.

1.2 Commissioner Manzie stated the document should include:

"a) The history of the missing laptops as known by the organisation to date

b) What connection there has been with the issue of child sexual exploitation

c) What actions were put in place by the organisation

d) The history and timeline of recent developments in relation to the media and what light it sheds on past events".

2 Information Obtained and Limitations

2.1 Information reviewed in this audit has been obtained from:

- The Freedom of Information Team
- The Press Office
- Corporate ICT
- Individual A
- Individual B
- Individual C
- Individual D
- The Casey Report.
- Anonymous letter received 26th September 2016

2.2 It is unlikely that this review will be based on a full record of every piece of information relating to this issue. Key people involved in the Council's response to the incident have now left the organisation, and it is likely they held some details that are not now available to the Council. The key people include:

- The former Director Safeguarding and Corporate Parenting, CYPS
- Individual F.

2.3 Details held by the Freedom of Information (FOI) Team appear comprehensive; there is a full trail of FOI requests received and the Council's responses and there is a full record of two reviews completed by the Information

Commissioner's Office (ICO). There are also records from the Team's work recording system of meetings and discussions held by Team members on the matter.

2.4 However, there are gaps in the details held by the Press Office, for example we do not have requests for comments to match statements made to the press in some instances, and in some cases we have draft statements but are uncertain whether these were issued or not.

3 Summary of the Incident and Actions Taken by the Council

3.1 On 26th October 2011, 21 laptops were stolen from the Council's Norfolk House Building, where staff within the CYPS Directorate were located. The stolen laptops belonged to the CYPS Safeguarding Unit, the Post Room, the Business Support Unit and the CYPS 'Right 2 Rights' Team. The laptops were not encrypted. They were password protected which provided a degree of protection, although it was thought the data held on the laptops would be fairly easily retrievable by anyone with reasonable ICT technical skills. It was found that 5 of the laptops contained personal data relating to Children, Adults and staff.

3.2 A number of actions were taken by the Council following the incident, including:

- Immediately, on 27th October 2011:
  - instigating an investigation into the incident and the risks to social care clients
  - reporting the matter to the Police
  - changing access codes for the Norfolk House building.
- Reminding all staff of the need for security and their responsibilities.
- Expediting the programme of encrypting laptops to substantially enhance security in the event of any future losses – the programme was completed by March 2012.
- Incorporating lessons with regard to building access into the design of the Council's new civic office; Riverside House, including the provision of personal lockers to avoid any laptops being left on desks overnight.

3.3 Individual E, Individual A and Individual F were asked to look into the incident and its implications, along with the teams suffering losses. Individuals E, A and F looked on the Council's network file storage – H:drive, which at the precise time of the theft contained a replica of the laptops' own hard drives, to establish what information was held on the laptops.

3.4 There were varying views about the volume and sensitivity of data lost, but it was ultimately accepted by the Council that there was some sensitive personal information on the laptops stolen.

3.5 Regrettably, a copy of the H:drive was not taken at the time of the theft, which meant that as soon as staff were given new laptops, re-connected to the network and used any of the files on the H:drive, this would have over-written the files and meant the Council lost any chance it had of taking a copy of the

precise data lost on the stolen laptops. In hindsight, the Council should have taken a full back-up of the H:drive for these laptops to hold a record of what was lost, but this was not done.

3.6 The Director of Safeguarding and Corporate Parenting stated in an email dated 12th December 2011:

- *"I shared the adult names with the Police … Their decision is not to inform the named adults on the list.*
- *I have discussed the children … and risk assessed the merit of telling some or all of the named individuals.*
- *In conclusion we felt it was in the interests of all the named individuals that they should not be informed".*

The Children and Adults who were referred to in the data held on the stolen files were not told that their data had been stolen.

3.7 Officers considered in considerable depth whether to report the theft to the ICO. A report produced for the Strategic Leadership Team (SLT) in the name of Individual B recommended not reporting the case to the ICO and this recommendation was followed. Although the Casey Report referred to a meeting of the SLT on 19th December 2011 (see extract at **Appendix 1**), the then Chief Executive's diary indicates that this meeting did not happen. Individual B states the decision was made prior to a formal SLT meeting and was not on the agenda, although he was unable to specify the meeting date. This audit has found no SLT minute confirming the decision.

3.8 An anonymous letter was received by the Council's Internal Audit Section, via the internal post system, on 22nd September 2016. Primarily the letter was reporting issues in respect of a client receiving care allowance, however, it also made specific reference to the theft of the laptops from Council Offices.

Whilst the letter did not specifically refer to Norfolk House, it referred to Council offices and theft of laptops containing vital information. In addition, the letter specifically named a person who was allegedly responsible for the theft. The named individual is not currently, nor has ever been, an employee of the Council.

3.9 The Council have liaised with South Yorkshire Police, who have made enquiries into the allegations. They have informed the Council that the anonymous allegation itself is not enough to obtain a search warrant. However, the person concerned had been under investigation for separate matters, which included searches of his premises. Laptops were not found in those searches, they are therefore confident that the laptops are not present at his address. The Council asked for a review of the police work and the findings were confirmed by the Divisional Commander.

4 Links with Child Sexual Exploitation and the Casey Report

4.1 A full copy of the H:drive of the stolen laptops was not made at the time of the theft and so it is not possible now to form a current view of the seriousness of data held on the laptops. Details of the reviews completed at the time are sketchy and not entirely consistent:

- Individual E stated in an email dated 1st November 2011: "*there are details of the sexploitation case involving taxi drivers. This includes names, addresses, birth dates of both the victims and the alleged perpetrators plus some narrative about the events"*
- The former Monitoring Officer stated in a response to the ICO dated 28th January 2013, "…*We believe information may have been passed to you from an employee who was subsequently moved to another role then made redundant* [Individual E]. *They were therefore not involved in the full enquiry and would not have been party to the final outcome".* (underlining by audit)
- Individual F who had also reviewed the H:drive stated at a meeting on 22nd November 2011 that there was a risk relating to, *"a copy of Strategy Minutes… provided the names of 19 children, 12 with addresses, the reasons why these children were linked to this case, and the names of 4 adults, with addresses…".* The officer also stated following their review, "*Overall, apart from this document, the feeling was that the situation, although serious with regard to the data loss, was not a significant risk with regard to access to details regarding vulnerable children".*
- In a letter to the Information Commissioner dated 11th April 2012, the Council concluded that none of the data found on the 5 laptops containing Children's or Adults information "*was sensitive personal data".*
- The ICO disagreed with the Council's assessment and, subsequently, in a letter to the Information Commissioner dated 28th January 2013 the Council accepted the Information Commissioner's view that *"… there was likely to have been 'sensitive personal data' involved".*

4.2 Reference to the theft of the laptops was included in the Casey Report. The full extract is included in Appendix 1. Key points in addition to what is already covered above, are:

- *"Inspectors were contacted by a former employee who alleged that the Council failed to inform the Information Commissioner's Office (ICO) about the loss of possibly '50% of children's data held by the Council at the time'*
- *The matter was discussed at a meeting of the Corporate Governance and IT Governance Board on 7th November 2011 chaired by ex-Councillor Jahangir Akhtar".*

This audit found no evidence from the information available or enquiries with current employees involved in the investigation at the time, to suggest 50% of Children's data was put at risk. The audit has also found no reference in any documentation provided by Corporate ICT and the Freedom of Information Team to any meeting of a Corporate Governance and IT Governance Board

held in November 2011, other than the reference within the Casey Report. Additionally, no-one interviewed during this audit was aware of such a meeting.

4.3 There were clearly varying views of the volume and sensitivity of data lost or exposed as a result of the incident. It is difficult to judge now without being able to go back to the original data, quite how much data was lost and how sensitive it was. It does appear strange though from what information is available, that the Council would try to suggest there was no sensitive personal data amongst the details lost. The Information Commissioner did not accept this and the Council ultimately conceded this point.

5 The Council's Response to the Information Commissioner, Press and Public Enquiries

Information Commissioner

5.1 The Information Commissioner has carried out two reviews of the incident. The first arose when the ICO's Office contacted the Council on 19th March 2012 after reference to the theft in an 'Advertiser' newspaper article dated 24th February 2012.

5.2 As part of its response to questions from the ICO, the Council confirmed, in a letter dated 11th April 2012, that the following was held on the laptops when they were stolen:

- *"brief notes of a meeting relating to a Police investigation into the exploitation of teenagers. The notes did not go into specific details but did contain the names of the persons concerned. In some cases dates of birth and address were also recorded. Inquiries established that only four of the named individuals are residing at the address at which they were residing when the notes were prepared".*
- *"letters from and to the Probation Service in respect of individuals' release dates from prison where they planned to reside in the Rotherham area".*

However, in relation to the information found, the Council stated "*None of the data was sensitive personal data*". This statement seems difficult to justify (paragraph 4.1 also refers)

5.3 The ICO asked the Council for its "*reasoning for not reporting the incident to the Commissioner at the time*", to which the Council responded; "

> *Given the difficulty of anyone other than an ICT specialist getting round the security measures on each laptop, …and having regard to the Commissioner's guidance on notifying him of data security breaches, the Council took the view that there was no clear purpose in informing the Commissioner of the loss as everything possible had been done to establish the nature of the data on the five laptops and necessary steps taken*".

5.4 On 21st June 2012, following its first review, the ICO concluded:

> ***"Consideration of the case***
> *The circumstances of this case are considered serious, and the failure*

of council staff to comply with its confidentiality and information security policies, resulted in the potential inappropriate disclosure of the information concerned…
From the information that you have provided, we have concluded that the type of data involved in this incident appears likely to be 'sensitive personal data',...

Decision of the Commissioner
The Commissioner has noted that the council had initiated a full encryption programme of all computers prior to the theft. It is my understanding that this programme has now been completed. It has also been recognised that a policy was in place which prohibited storage of personal data on the hard drive of computers…
Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion".

5.5 The ICO Office contacted the Council again on 20th December 2012 instigating a new review and stating the reason for this as "*The ICO is now in receipt of further information that relates to this matter …".* The ICO asked for detailed information linked to the incident and the Council provided responses to the questions asked. The Council also stated on 28th January 2013, as part of its responses to the ICO; "*Whilst we have not found any evidence that the laptops stolen on 27/10/2011 contained any sensitive data we accept your conclusion of the 21/06/2012 that there was likely to have been "sensitive personal data" involved*".

5.6 A conclusion was received from the ICO on 13th May 2013, which was "*…it has been decided that no further action is necessary in this instance. This is on the basis that a full encryption programme has been completed for mobile devices to mitigate any future risk.*

As such the case will now be considered as closed…

5.7 On 18th March 2015, the ICO notified the Council that it had received a Freedom of Information request for all correspondence relating to the laptop thefts of October 2011 and identified the documents to be provided, including RMBC internal emails, some of which are referred to within this report.

Press Enquiries

5.8 The Council received a general enquiry (by way of a Freedom of Information request) from the Advertiser Newspaper on 28th December 2011 for "*Details of all Rotherham Borough Council property reported lost or stolen since the beginning of 2011…*". The Council provided details in response, which included reference to the stolen laptops and this culminated in the article in the Advertiser dated 24th February 2012 (paragraph 5.1 refers).

5.9 A further request from the Advertiser led to a statement being prepared by the Council on 12th September 2014, which included, "… *of the 21 stolen laptops, three contained personal data relating to children known to social services.*

However, copies of this documentation is not held by the Council and so we are unable to confirm the exact detail of the content." The press may have taken this to mean the Council stated it was not aware what data was on the laptops because an article run by the Advertiser on 7th November 2014, stated "… *council officials have claimed they do not know what information was on 21 laptops stolen from council offices, amid claims they allegedly contained details of child sex abusers and victims".* It is not known who or what the source of the "*claims*" made to the Advertiser was.

5.10 I cannot see anywhere that the Council has actually stated that it did not know what information was held on the laptops. However, the wording used by the Council in its statement of 12th September 2014 was far from clear and reflected the evasive way in which it has dealt with this issue.

5.11 Following the release of the information held by the ICO (see paragraph 5.7), the Council was contacted by the Sheffield Star Newspaper and the Advertiser about the details within the information they had now seen demonstrating the Council was aware of the information contained on the stolen laptops. Both ran articles in September 2015 criticising the Council for its lack of openness regarding the incident.

Enquiries from the Public

5.12 Four Freedom of Information requests have been received from members of the Public.

5.13 A review of the questions received and response given showed the Council could have been more comprehensive and helpful in its responses. For example:

- One request asked for "*copies of minutes of any meetings or reminders held / sent after the theft of laptops that reminds staff not to store sensitive data on C drive*", and also asked the Council to "*confirm who reported the data loss to the Information Officer and on which date, specifically, did the council themselves report the loss to the Information Officer or was the Information Officer made aware from another source?*". A response is provided but again it is not forthcoming; it stated "*Discussions were held regarding the theft but there was no formal minutes recorded*". Whilst it may be true there were no "formal minutes", there were nonetheless notes of the meetings, which this audit has seen.
- One question asked whether "*all laptops provided were equipped with encryption ability …",* to which the Council responded *"Yes, Rotherham MBC can confirm that laptops were issued with encryption ability".* While this was true and answered the specific question asked, it did not state the encryption had not actually been activated on the stolen laptops at the time of the theft.

5.14 Overall, the audit found the Council's responses to questions from the Press and Public were cautious and not completely open.

6 Conclusions

Key issues

6.1 The key points at issue in this report are whether in the light of recent press enquiries, the Council has been accurate in its declarations about the theft of the 21 laptops in 2011:

- To the Information Commissioner?
- To the Press?
- In response to Freedom of Information enquiries?

Key facts

6.2 Key facts are that:

- While council staff accessed the data initially on the reporting of the theft, they did not take the necessary steps to secure a permanent copy of the data which was on the stolen laptops.
- There were varying views amongst different council staff as to the sensitivity of the data on the laptops. The fundamental question of the extent to which sensitive safeguarding information was put at risk is difficult to judge after the passage of time without being able to go back to the original data.
- A decision was taken by staff who no longer work for the council not to disclose to the small number of adults whose data had been on the laptops the fact that the laptops had been stolen.
- These staff similarly decided not to disclose to the small number of young people whose data had been on the laptops that the laptops had been stolen.
- The then Strategic Leadership Team agreed not to report the loss of the laptops to the Information Commissioner.
- The ICO was only informed of the data loss on his initiative following an article in the Rotherham Advertiser on 24th February 2012 about the theft of the laptops. This led to two investigations by the ICO at the end of which he concluded no action was needed and the matter to be closed.
- The Council's responses to the Information Commissioner were not always complete and instructive, and, after initially suggesting there was no sensitive personal data lost, subsequently agreeing with the ICO's view that it was likely there was.
- An anonymous letter has named an individual allegedly responsible for the theft of the laptops, however that individual had been investigated by the police under separate investigations and they are confident that the laptops are not present at his address. The named individual is not currently, nor has ever been, an employee of the Council.

Conclusions

6.3 The Council has not handled the matter well; it failed to take steps to secure the data lost, made a doubtful decision to not report the matter to the Information Commissioner and has been less than helpful in responding to ICO, Press and Public enquiries. Taken together, it is understandable that others have formed a view that the Council has covered-up the facts.

6.4 The audit found no factually inaccurate statements made by the Council.

With Reference to the Information Commissioner

6.5 The Casey Report concluded "*Whilst it is not possible to prove exactly what was held on the H drive and therefore what was lost, evidence seen by the Inspectors confirms that the Council did cover up the scale of the loss known at the time*". The evidence for this is in the then SLT's decision not to inform the Information Commissioner of the loss at the time. It was an error to not report the incident to the ICO. This would have been the right thing to do, and had the management team reported in full what had happened at the time, the opportunity for the accusation of "cover up " would not have been possible to make, unless inaccurate information was supplied.

6.6 It is a confirmation of the failures in corporate governance at the time that despite genuine efforts by a number of people to track the formal decision not to inform the Information Commissioner, and although the report dated 19th December 2011 appears to be the basis on which the decision was taken, officers cannot find any formal minute. It is said that the decision was taken in an informal discussion before an SLT, which we have not yet been able to trace. Equally this audit has found no record of any Corporate Governance and ICT Board meeting that was reckoned to have taken place on 7th November 2011.

With Reference to enquiries from the Press and Public

6.7 In relation to the accuracy of responses to the press and freedom of information enquiries, this audit has concluded Council staff have given factual statements to the press and in relation to Freedom of information enquiries, but their failure to give a full explanation of events has meant the Council has been less than open. In particular

- When asked by the Press, the Council has stated that it did not have a copy of the data on the stolen laptops, although it has stated that it saw and reviewed the data that was held at the time (ie. it saw and reviewed the data held on the H;drive immediately following the theft). It did not, however, explain the technical point that staff had seen the data but then failed to take a copy of it or the implications of it. This meant that the explanation sounded as though it was either not true or indicated failures to take appropriate action. In fact it did indicate a failure to take appropriate action.
- One Council response stated that the laptops had the capacity to be encrypted but it did not go on to provide the important fact that although

they had such capacity they were not actually encrypted and the time of the theft.

7 Recommendations

7.1 The key recommendations now are that the Council:

i) Reports all significant data losses to the Information Commissioner promptly and fully

ii) Immediately files a record of whatever data is lost via a data security breach so that there is clarity about the data loss

iii) Organises its handling of corporate data breaches in an appropriate way through the Data Controller and the Monitoring Officer

iv) Continues to provide regular training in data security

v) Answers all future enquiries into the theft of the laptops as fully as possible

vi) Reminds all staff of the information security policy and their responsibilities relating to it at regular intervals

vii) Ensures all information relating to press requests for statements is retained

viii) Writes to Louise Casey CBE and briefs Commissioner Ney (formerly of the Casey inspection team) to explain that this further review has been done and its relevance to the Casey Report.

8 External Opinion by insight Investigations

8.1 Insight Investigations were commissioned by Rotherham Council to conduct a critical and independent review of Internal Audit's work. Insight Investigations reviewed Internal Audit's report following its work, examined Internal Audit's working papers and questioned Internal Audit about its work. Insight Investigations have confirmed that:

- Internal Audit has carried out all reasonable tests available to it in relation to this matter and its work completed on these tests was comprehensive, and that
- The conclusions reached by Internal Audit are accurate and reasonable, based on the work completed and the information available to them at that time.

8.2 The full opinion of Insight Investigations follows.

Insight Investigations

Please reply to our Head Office
Our Ref: TS/NS/44030
16th February 2017

STRICTLY PRIVATE AND CONFIDENTIAL
TO BE OPENED BY ADDRESSEE ONLY
[redacted]
Head of Internal Audit
Finance & Customer Services
Rotherham Metropolitan Borough Council
Main Street
Rotherham
S60 1AE

Dear [redacted]

Review of Internal Audit Work – the Council's response to the theft of 21 Laptops from Norfolk House, Rotherham: 26th October 2011

I am writing to you in relation to Insight Investigations' review of Internal Audit's work into the Council's response to the theft of 21 Laptops from Norfolk House, Rotherham: 26th October 2011. Internal Audit was instructed by Rotherham Council to establish:

- What enquiries were made by the Council regarding the theft of 21 Laptops from Norfolk House, Rotherham on 26th October 2011. To include the history surrounding the security of the laptops and their data, any connections to the issue of child sexual exploitation, actions that were put in place by the Council and the history and timeline of media communications.

The terms of reference agreed between Rotherham Council and Insight Investigations required Insight Investigations to conduct an independent review of Internal Audit's work:

- To determine whether the work carried out by Internal Audit was comprehensive taking into account any limitations in the authority and powers of the Internal Audit Service, or whether there was any further work that should be carried out.

- To determine whether (or not) the conclusions drawn from the work carried out were reasonable conclusions to reach (i.e. would we agree with those conclusions).

Insight Investigations have reviewed Internal Audit's report following its work, examined Internal Audit's working papers and questioned Internal Audit about its work. On the basis of this review, I am able to confirm Insight Investigations' opinion, which is:

- Internal Audit has carried out all reasonable tests available to it in relation to this matter and its work completed on these tests was comprehensive, and that

- The conclusions reached by Internal Audit are accurate and reasonable, based on the work completed and the information available to them at that time.

Insight Investigations is a private investigation service with over 30 years of experience of private, commercial and corporate investigations. The company was commissioned by Rotherham Council to conduct an independent, objective review of the work of its Internal Audit Service.

Assuring you of our utmost attention at all times.

Yours sincerely

[redacted]

INSIGHT INVESTIGATIONS

Appendix 1: Extract from the Casey Report

Extract from the Casey Report (Feb 4th 2015)

The Case of the Missing Laptops

Inspectors were contacted by a former employee who alleged that the Council failed to inform the Information Commissioner's Office (ICO) about the loss of possibly '50% of children's data held by the Council at the time'. The data was held in the 'H cache' of 21 laptops that were stolen from RMBC on 26th October 2011.

Inspectors reviewed all information the Council held in relation to this matter. The uncontested facts are that:

- there was a theft of 21 laptops from Norfolk House on the night of 26th October 2011
- there was no sign of a break in
- there was an investigation
- there was a report to Senior Leadership Team
- the Council did not alert the ICO
- the Council responded when the ICO wrote to them, on two occasions.

The Council admitted that some sensitive data was lost, including that relating to victims of CSE. The investigation report shows that the matter was discussed with the police and information relating to CSE was present on the laptops, including the names of adults who may have been offenders. This much is agreed between the whistle-blower and the Council. But what is in contention is what else was on the lap-tops.

The whistle-blower asserts that a large volume of other sensitive children's data was lost. He says the matter was discussed at a meeting of the Corporate Governance and IT Governance Board on 7th November 2011 chaired by ex-Councillor Jahangir Akhtar. The meeting was told that a report recommending that the data loss should not be reported was being prepared for the Senior Leadership Team.

The risk of a hefty fine from the ICO was the key consideration at the time.

The Council does not have the minutes of this meeting. Inspectors reviewed a report prepared for SLT on 19th December 2011. This confirms the whistle-blowers testimony, including the loss of sensitive data.

'It is understood that some of the laptops may have had sensitive information stored on the computer's in-built hard drive (known as the 'C:\ drive') which includes the user's desktop. In addition, information held on the H:\ drive will have been 'cached' (copied) to the C:\ Drive to facilitate offline working…'

Due to the sensitivity of the information, it may be necessary to inform the Information Commissioners Office of the data loss'.

The SLT report considers the risks relating to the loss, including: 'The safety of vulnerable persons, particularly children, could be compromised if the information is accessed. The Council could also fail to meet certain statutory obligations in relation to safeguarding vulnerable children or adults.'

The SLT report concludes:

'If we report this breach to the ICO it is likely that we will have to sign a formal undertaking to encrypt all portable and mobile devices used to transmit personal information. We may also be fined for the breach. The ICO can now impose fines of up to £500,000.'

The whistle-blower alleges that he demonstrated how easy it was to get access to these laptops. He had spent two hours on Google to work out how to get into them without a password, and he proved it could be done.

There is no minute of the 19th December SLT so we do not know whether the matter was discussed. Either way, the Council did not report the loss. The ICO became aware of it from an article in the local Advertiser, which reported the theft but did not pick up on the data issue. In response to the ICO's enquiry, in June 2012, the Council advised him in summary that 'none of the data was sensitive personal data'.

This was accepted by the ICO. However further information comes to his attention and he writes again. This time the Council is more specific about what is held but again they do not reveal the extent of the loss in terms of the cached H drive. Even so the ICO concludes that:

'the type of data involved in this incident appears likely to be "sensitive personal data"... and has the potential to cause significant detriment to the individuals concerned if compromised…We welcome the remedial steps taken by the Council in light of this incident...Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion.'

Whilst it is not possible to prove exactly what was held on the H drive and therefore what was lost, evidence seen by Inspectors confirms that the Council did cover up the scale of the loss known at the time.

The whistle-blower claims that as a result of his persistence in raising the loss, he was restructured out of a role in a restructure of IT services. Our checks show that he was unsuccessful in securing a job in the restructure of IT, no suitable offer of alternative employment could be found at the same grade, he turned down demotion and was therefore made redundant.