

**THE SOLICITORS (SCOTLAND) ACT 1980  
THE SCOTTISH SOLICITORS' DISCIPLINE TRIBUNAL  
(PROCEDURE RULES 2008)**

**INTERLOCUTOR**

in Complaint

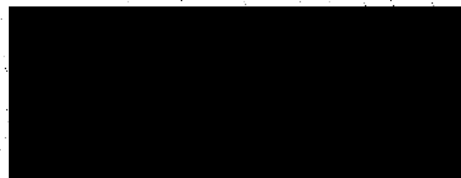
by

THE COUNCIL OF THE LAW SOCIETY OF  
SCOTLAND, Atria One, 144 Morrison Street,  
Edinburgh (hereinafter referred to as "the  
Complainers")

against

KEVIN FREDERICK MACPHERSON,  
Ravenswood House, PO Box 9945,  
Stornoway, Isle of Lewis, Solicitor  
(hereinafter referred to as "the Respondent")

Edinburgh 19 June 2019. The Tribunal having considered the Complaint at the instance of the Council of the Law Society of Scotland against Kevin Frederick MacPherson, Ravenswood House, PO Box 9945, Stornoway, Isle of Lewis; Repels the Respondent's first and second pleas-in-law; Reserves the question of expenses until the conclusion of proceedings; and Continues the Complaint to a hearing to be fixed.



**Alan McDonald**  
**Vice Chair**

**THE SOLICITORS (SCOTLAND) ACT 1980  
THE SCOTTISH SOLICITORS' DISCIPLINE TRIBUNAL  
(PROCEDURE RULES 2008)**

**FINDINGS** following a preliminary hearing

in Complaint

by

**THE COUNCIL OF THE LAW SOCIETY of  
SCOTLAND, Atria One, 144 Morrison Street,  
Edinburgh**

**Complainers**

against

**KEVIN FREDERICK MACPHERSON,  
Ravenswood House, PO Box 9945, Stornoway,  
Isle of Lewis**

**Respondent**

1. A Complaint was lodged with the Scottish Solicitors' Discipline Tribunal by the Council of the Law Society (hereinafter referred to as "the Complainers") averring that Kevin Frederick MacPherson, Ravenswood House, PO Box 9945, Stornoway, Isle of Lewis (hereinafter referred to as "the Respondent") was a practitioner who may have been guilty of professional misconduct.
2. There was no Secondary Complainer.
3. The Tribunal caused a copy of the Complaint as lodged to be served upon the Respondent. Answers were lodged for the Respondent.
4. In terms of its Rules, the Tribunal fixed a procedural hearing for 13 September 2018 and notice thereof was duly served upon the Respondent.
5. At the procedural hearing on 13 September 2018, the Complainers were represented by their Fiscal, Grant Knight, Solicitor, Edinburgh. The Respondent was absent but was represented by David Burnside, Solicitor, Aberdeen. The Tribunal ordered that the procedural hearing should be heard in private in terms of Rule 43 of the Scottish Solicitors'

Discipline Tribunal Rules (hereinafter referred to as "the Rules") using the dispensing powers of the Tribunal under Rule 47. Both parties invited the Tribunal to fix a preliminary hearing to take the form of a debate. The Tribunal fixed a preliminary hearing for 12 December 2018 and ordered that it should be held in private.

6. On 26 November 2018, due to the terms of the notes of argument which were produced by parties, the Vice Chair, exercising the functions of the Tribunal under Rule 56, converted the preliminary hearing fixed for 12 December 2018 to a procedural hearing to determine the appropriate further procedure.
7. At the procedural hearing on 12 December 2018, the Complainers were represented by their Fiscal, Grant Knight, Solicitor, Edinburgh. The Respondent was not present but was represented by David Burnside, Solicitor, Aberdeen. The Fiscal made a motion for the hearing to be fixed and the issue of admissibility of evidence to be decided at that full hearing in the form a proof before answer. Mr Burnside moved the Tribunal to fix a preliminary hearing to deal only with admissibility of evidence with further procedure to be determined thereafter. The Tribunal granted the Respondent's motion and fixed a preliminary hearing for 26 April 2019 for the Tribunal to consider admissibility of evidence. The Tribunal granted the Respondent's motion for the preliminary hearing on 26 April 2019 to be heard in private.
8. Prior to the preliminary hearing on 26 April 2019, the Complainers and the Respondent were allowed to amend the Complaint and Answers respectively. A Record was produced.
9. On 26 April 2019, the Complainers were represented by their Fiscal, Grant Knight, Solicitor, Edinburgh. The Respondent was present and represented by David Burnside, Solicitor, Aberdeen. Mr Burnside led evidence from the Respondent. Mr Knight led evidence from three witnesses. There was insufficient Tribunal time to deal with the parties' submissions on the pleas-in-law. Therefore, the Tribunal continued the preliminary hearing to 19 June 2019.
10. On 19 June 2019, the Complainers were represented by their Fiscal, Grant Knight, Solicitor, Edinburgh. The Respondent was not present but was represented by David Burnside, Solicitor, Aberdeen. Parties made submissions.

11. Having heard evidence in respect of the Respondent's pleas-in-law the Tribunal found the following facts established:-

11.1 The Respondent is a solicitor enrolled in the Registers of Scotland. He was enrolled as a solicitor on 9 November 1988. He is the principal of Kfm Law, Ravenswood House, PO Box 9945, Stornoway, Isle of Lewis. He was previously a partner in the firm of Ken MacDonald and Co, 9 Kenneth Street, Stornoway, Isle of Lewis from 1 April 2009 until 30 November 2012, and thereafter a director of Ken MacDonald and Co. Limited trading from the same address, from 1 December 2012 until 30 August 2013 (hereinafter referred to as "the firm").

11.2 On 14 March 2011 following upon an offer made by the Respondent, the said firm engaged a trainee solicitor (hereinafter "TS"). The Respondent was the supervising solicitor for her traineeship. The said TS subsequently qualified as a solicitor on 13 March 2013 and remained in the employ of the said firm until 30 August 2015.

11.3 On 28 May 2013 the office manager employed by the said firm (hereinafter "Mr B") accessed a computer operated by the Respondent within the said firm's offices. On that computer were found a number of emails covering a period from 8 April 2011 to 22 June 2012, certain of which made reference to the said TS. Said emails were exhibited by the said office manager to TS who became distressed at their content. On 31 May 2013 the said emails were exhibited to the other Partner within the said firm and the fellow director of the Respondent within the said firm.

Mr B was employed by the said firm on 11 June 2007 as Office Manager and Legal Assistant. His duties as Office Manager included dealing with staff issues, office equipment, the maintenance and administration of the firm's IT systems, and generally administering the firm's offices. The IT system and network within the said firm was operated with passwords but most computers on the network could easily be accessed by any member of staff. When opened, the desktop on each computer would appear. Each computer was ordinarily used by the individual at whose desk it was situated. Each user had the facility to store data on their own computer. Each user had their own email icon on their desktop with their

individual email address set up within that icon. The said firm used Microsoft Outlook. Each user's email account was not password protected. When solicitors or fee earners were absent from the office on business or on holiday, other members of staff generally had access to their computer to check, monitor, and where appropriate respond to, emails. In addition, if documents were stored on a computer's individual hard drive, other members of staff could access that computer to open such a particular document. The Respondent's computer was accessible without using a password. On or about 28 May 2013, Mr B accessed the Respondent's computer. He looked at the Respondent's email inbox. Said inbox was open and neither locked nor protected by a password. He found emails which are the subject of part of the Complaint against the Respondent. He printed copies of the same and gave them to TS and another solicitor in the firm and eventually to the other director.

On 28 May 2013, there was no information security policy in force at the firm. There was no physical or policy barrier preventing access to the Respondent's computer and his emails.

12. Having heard submissions from both parties, the Tribunal repelled the Respondent's pleas-in-law and determined that the emails in question were admissible and should be admitted to probation at the hearing on professional misconduct.
13. The Tribunal pronounced an Interlocutor in the following terms:-

Edinburgh 19 June 2019. The Tribunal having considered the Complaint at the instance of the Council of the Law Society of Scotland against Kevin Frederick MacPherson, Ravenswood House, PO Box 9945, Stornoway, Isle of Lewis; Repels the Respondent's first and second pleas-in-law; Reserves the question of expenses until the conclusion of proceedings; and Continues the Complaint to a hearing to be fixed.

(signed)

**Alan McDonald**  
**Vice Chair**

14. A copy of the foregoing together with a copy of the Findings certified by the Clerk to the Tribunal as correct were duly sent to the Respondent by recorded delivery service on 13 August 2019.

**IN THE NAME OF THE TRIBUNAL**



**Alan McDonald**

**Vice Chair**

**NOTE**

This decision relates to procedural and preliminary issues which arose before the Complaint was set down for a hearing. At the procedural hearing on 13 September 2018, the Tribunal fixed a preliminary hearing for 12 December 2019. The preliminary hearing was to take the form of a debate. Due to the terms of the notes of argument produced by the parties, it became apparent that evidence might require to be led as there was no agreed factual position. Therefore, the preliminary hearing fixed for 12 December 2018 was converted to a procedural hearing to determine the appropriate further procedure.

On 12 December 2018, the Respondent's agent moved the Tribunal to fix a preliminary hearing to deal only with admissibility of evidence with further procedure to be determined thereafter. The Complainers moved the Tribunal to fix a hearing to take the form of a proof before answer. Both parties made submissions in support of their motions. The Tribunal considered that holding a proof before answer could potentially prejudice the Respondent. The Complaint alleged misconduct in relation to TS which was separate to the alleged conduct in relation to the emails. It was therefore in the interests of fairness for the admissibility of the emails to be determined separately and prior to the rest of the Complaint. If the Respondent was successful in his motion to have the emails excluded, a fresh Tribunal could consider those aspects of the Complaint without being influenced by the terms of the emails. Holding a proof before answer would also force the Respondent to answer all aspects of the Complaint together and this might be prejudicial to his defence. The Tribunal took into account the inconvenience to the Complainers' witnesses and the Tribunal as well as the inevitable delay which would follow a decision to determine the admissibility question prior to the hearing on the Complaint. However, the Tribunal considered that the balance of fairness was in the Respondent's favour. Therefore, it granted the Respondent's motion and fixed a preliminary hearing for 26 April 2019 for the Tribunal to consider admissibility of evidence. The Tribunal granted the Respondent's motion for the preliminary hearing on 26 April 2019 to be heard in private.

The preliminary hearing took place over two days. On 26 April 2019 and 19 June 2019, the Tribunal had before it the Record dated 8 April 2019, Notes of Argument for the Respondent and Complainers, a list of authorities for the Respondent, a list of witnesses for the Complainers, two lists of productions for the Complainers and two lists of authorities for the Complainers. Between 26 April 2019 and 19 June 2019, parties provided written submissions.

## EVIDENCE OF THE RESPONDENT

The Respondent gave evidence on oath. He became an office junior at Ken MacDonald & Co in 1997 and started his traineeship in October 1997. He progressed to associate and partner. He was partner from 1 April 2009 until November 2012. He had a general practice. He never had a contract of employment. He did not think any employee had one. He had a good relationship with Mr MacDonald. He was aware of Mr B's appointment in Summer 2007. Mr B was appointed as a legal assistant or secretary to Mr MacDonald.

The Respondent was referred to Production 1/1 in the Second Inventory of Productions for the Complainers, which bore to be Mr B's employment contract. The Respondent indicated that he first saw this document as part of the preparation for the present case. It was signed on the same day he became partner, which was also the start of the financial year. The Respondent said Mr B did not carry out the duties of office manager. He did not deal with the issues listed in article 2.3 of the Complaint, namely dealing with staff issues, office equipment, the maintenance and administration of the firm's IT systems and general administering of the firm's offices. The Respondent said that the cashier, carried out these functions. She was the "unofficial office manager".

When absent from the office, the Respondent could access emails on a BlackBerry smartphone. He had a desktop computer in the office. It was not password protected. He did not recall ever having to use someone else's computer. He had no knowledge of anyone else accessing his computer. There would not be any need to do so. He worked lengthy hours and had email access 24/7. The firm still used paper files. He accepted there was nothing to prevent someone else accessing his computer. However, he never gave anyone permission to do this. He would expect staff to try and contact him first. For example, when absent from the office, he would throughout the day receive emails regarding queries which had been made to the office by telephone. It was the Respondent's usual practice to use his work email system to send personal messages. He "*treated professional and personal just the same*". He would not mark personal emails as private. He never had any concern that anyone would access his emails.

The Respondent was aware of the terms of the Complaint which alleged that Mr B accessed his computer in or around December 2012. The Respondent was present in the office during this period except for his monthly overnight visit to Lochmaddy Sheriff Court. He had a big transaction settling at this time and was rarely away from the office. The Respondent said that all his files and styles were kept on his pen



drive as he worked a lot at nights and weekends. No other versions were stored on his computer at work or at home. If Mr B needed to look for a deed, he should have contacted the Respondent. Mr B did not work as the Respondent's assistant. He did not know anything about the Respondent's transactions.

The Respondent denied the suggestion that he kept pornography on his computer. He said this was untrue and that he had no recollection or knowledge of discussing this matter with Mr B. There was no conversation between them about this. Any such statement would be untrue. If he had been caught with pornography, he would have removed it immediately. However, it did not happen.

Turning to the circumstances surrounding Mr B's alleged second access to the Respondent's computer in May 2013, the Respondent explained that a new online banking system was introduced in the firm in February or March 2013. The bank's policy was to send information by post for fraud or security reasons. All online banking material was kept together in the cashier's folder. The Respondent and Ken MacDonald were "administrators" of the online banking system. The Respondent and Mr C were "users". Users could authorise payments. Administrators could determine what could be done, who could make payments, the number of people needed to authorise payments, the level of payment which could be made etc. Staff using the online banking system had smartcards and card readers. Administrators and users had different cards. Any member of staff could create a payment but it had to be authorised by the Respondent, Ken MacDonald or Mr C. If there was a problem, the administrator would have to resolve it. However, the Respondent said there would not be anything on his computer which would assist. He resolved problems by using the bank's telephone helpline. It was untrue to say that Mr B knew that the Respondent had been in email contact with the bank.

It was suggested that it appeared Mr B was looking for a female name in the Respondent's inbox and came across the relevant messages there. The Respondent said he had not given Mr B permission to access his emails. The Respondent expected his emails to remain private as they belonged to him. The Respondent noted that Mr B did not discuss the emails with him or Ken MacDonald but went to another member of staff. Ken MacDonald came to discuss the matter with the Respondent on the Friday following their discovery on 28 May 2013. The Respondent decided to resign the following Monday. He worked his period of notice until the end of August.

Mr Burnside referred the Respondent to Production 9/2 in the Second Inventory of Productions for the Complainers. The Respondent indicated that he had first seen this information security policy when preparing for the present case. It was not in force when he was at the firm. There was no policy at that time.

The Respondent said that he did not give authorisation to anyone access his computer. If staff were doing so, he did not know they were doing it. The trainee had her own caseload and was not involved in his conveyancing. Mr Burnside noted that it would be normal for a trainee to deal with things in a supervisor's absence and might look at that person's computer. The Respondent said he would email the trainee or give her a file to deal with. She was not acting as his secretary or assistant on his cases. She had her own set of files. They were different fee earners for the cash room.

The Respondent said he received about 500 emails a month. He knew that Mr B described finding an email from January 2012. This would involve looking through 10 or 12 months of 500 emails a month. He has never understood how these emails were chanced upon.

### **CROSS-EXAMINATION OF THE RESPONDENT**

The Respondent agreed that he was challenging the admissibility of emails. Mr Knight asked him why he had chosen to do that as part of these proceedings. The Respondent indicated that he had always queried the competence of the emails. The Respondent confirmed that the Scottish Children's Reporter Administration (SCRA) became aware of these emails and investigated. He did not challenge admissibility because he was not involved in that investigation. The matter was referred to the Scottish Legal Aid Board (SLAB) and he was involved in that investigation. He raised issues of competence, admissibility and fairness. However, this issue was not taken up by his representative at that time. He was removed from SLAB work. The emails had been used by the SLCC and the Law Society during their investigations. He questioned their admissibility in consultation with his solicitor. In response to further questioning by Mr Knight, the Respondent indicated that the current objection was the first one taken in any of these proceedings.

In December 2012 the Respondent and Ken MacDonald were the sole directors and shareholders of the company. The firm did not have any formal security or monitoring policy for emails. If it had needed one, it is likely that the Respondent was the person who would have drafted it. However, it did not occur to him to formulate a policy.

The Respondent gave evidence that the firm's computers had no passwords. Anyone could open any computer. The firm operated on trust but people should not invade others' privacy. It did not occur to him that anyone would go into his emails. Mr Knight suggested that the generic password to open the network was "letmein" but the Respondent said he was not aware of that and he just used to press "enter".

The Respondent said he was not aware of anyone in the firm installing a password. If a solicitor or a member of staff had wanted to do that, that would not have been prohibited. The situation never arose. If a person had accessed his computer, they had no authority to do so. However, he never indicated to staff that they did not have his permission to use his computer.

Mr Knight noted in the Answers that it is positively stated that Mr B was not employed as the office manager on 28 May 2013. The Respondent confirmed that was still his position. Mr Knight referred the Respondent to Production 1 in the Second Inventory of Productions for the Complainers, Mr B's contract. The Respondent agreed that Mr MacDonald's signature was present on the document and that it was signed on the same day the Respondent was assumed as partner. Mr Knight said that it was strange that his partner had assumed an employee without telling him. The Respondent said that the only time contracts were discussed was when the company was incorporated.

The Respondent agreed that Production 2 in the Second Inventory of Productions for the Complainers was a letter to Mr B on 26 November 2012 advising him that the firm was being incorporated. He agreed that the letter had been signed by him and referred to a contract of 1 April 2009. The Respondent said he signed a letter like this for all staff. Mr Knight suggested that the documents implied that Mr B continued to work as office manager as per his contract. The Respondent said that his roles, activities and workload were not that of an office manager. However, he agreed that Mr B had a contract to that effect.

Mr Knight quoted from the Answers submitted on behalf of the Respondent as follows:-

*"The Respondent understands that the purported reason for the said Mr B accessing the Respondent's computer is to check for an email from the firm's bank. If that is contended, it is a false claim."*

The Respondent confirmed that he still maintained this was a false claim. If the Tribunal heard evidence to that effect from Mr B then he was lying. The Respondent said there had been no arguments between himself and Mr B. He thought that they had got on.

Mr Knight referred the Respondent to Production 3 in the Second Inventory of Productions for the Complainers, an application for online banking for a limited company. The Respondent said he had seen the document before. Mr Knight noted that the primary contact was the cashier and she had provided an email address. The Respondent said nevertheless, the bank never sent him any emails. All correspondence was by post. He agreed that his details as administrator were contained on page 3/4. Ken MacDonald's details were on page 3/5. Mr MacDonald did not use email. If he needed to send an email, he would use the cashier's email address or the generic email address. Mr Knight asked whether Mr

MacDonald was a computer enthusiast and the Respondent said that he was not. The Respondent confirmed that on page 3/6, Mr C's details as user are contained including an email address. The Respondent confirmed that there were two administrators and three users. The Respondent said that Mr MacDonald's pass and card reader were kept by the cashier in the cashroom. However, she never used them. Only Mr C and the Respondent dealt with the online banking.

Mr Knight referred the Respondent to Production 4 in the Second Inventory of Productions for the Complainers, an email from the Bank of Scotland to the cashier. The cashier was the principal point of contact for the firm. However, she was not able to act as an administrator. The Respondent disagreed with Mr Knight's suggestion that in practice she might have used Ken MacDonald's card. Mr C was able to sign cheques and do online banking. He has since passed away. The company needed someone other than the Respondent to be an administrator. Ken MacDonald was absent from the office frequently. They trusted Mr C. However, he could not deal with any online banking problems because he was not an administrator. He could make payments but could not set up the system. The online banking software was installed on the Respondent's computer and Mr C's computer. The online banking involved going through a website. That could be done from anyone's PC. The card reader could be moved to another computer. It was plugged into a computer with a USB lead. The Respondent was not aware of any problems with the computers or card readers. However, if a computer was not working it would be possible to use another computer. If the card reader was not working, it would be possible to take the Respondent's and use another computer or go online. Mr Knight asked whether Mr B's explanation was reasonable. The Respondent said it did not make sense to him. There was nothing on the PC or the emails to assist him or Mr C.

The Respondent said he did not know why the Answers described Mr B's access of the relevant emails on 28 May 2013 as "a systematic search". He did not know how long it would take to find the emails. Mr Knight asked whether it was possible that Mr B had made an error about the information available on the Respondent's computer. The Respondent said Mr B could have thought that. However, he did not think it was credible. Mr Knight asked how Mr B would know there was no useful information on the Respondent's computer. The Respondent said that even if there were bank emails, Mr B could not have done anything about it because he was not an administrator of the system. Mr Knight noted that there was a card in the cashroom. The Respondent said he would hope that Mr B would run it by him first before using that card.

The Respondent said that if the Tribunal heard evidence from Mr B that he had found pornography on Mr B's computer in December 2012 and spoken to him about it, he would be lying. He did not know why Mr B would lie.

The Respondent said that to his knowledge the bank had not suggested that the company required an information security policy. The Respondent agreed that if there was no policy in place and no contracts of employment and an open/trusting approach, members of staff did not know that they were not allowed to access his computer. However, he trusted them not to do it.

The trainee with the company in 2013 had her own office. She worked with the Respondent in his room on occasion. However, there was no occasion when she accessed his computer. It was possible that she could have done so when he was absent but he had no knowledge of this happening. Even if she had done so, he said there was a difference between looking for a style or a document and searching a sent email folder 10 or 12 months back.

The Respondent agreed that he considered the recovery of the emails in question an invasion of his privacy. He is aware of Article 8 and has seen the material provided to the Tribunal by his solicitor. He has never had cause to consider Article 8 for a client. Mr Knight asked whether he considered the trainee's rights to have been infringed. The Respondent said he never deemed those emails to be made public. He would never have made them public. Mr Knight noted that despite this, they had entered into the public domain. The Respondent said that this had happened due to the trainee's actions and they had used by other bodies.

## **RE-EXAMINATION OF THE RESPONDENT**

Mr Burnside asked how long Mr B would have to spend looking through the Respondent's emails before finding the ones in question. The Respondent said he assumed it would take some time if he was looking back through a history of 10 to 12 months. The Respondent received roughly 500 emails a month. The recipient of the emails had not given her permission for them to be used.

In response to questions from a member of the Tribunal, the Respondent indicated that the office used the Outlook email system. He said that no emails were ever deleted and they were not organised into folders. His emails went back to 2001. The Respondent said the recipient of the emails had no business with anyone else in the firm.

## EVIDENCE OF TS

The witness chose to affirm. Her address was care of her employers. She was employed by that organisation in August 2015. The witness did her traineeship with Ken MacDonald & Co, starting in March 2011. The Respondent was her supervising partner. She had her own office and computer. It was a basic PC. She would log into this with the password 'letmein'. She did not pick this password. She had cause to work with the Respondent in his room. This would happen several times a day. Her office was in a portacabin separate from the main building. His room was upstairs in the main building.

The witness said Mr B's role in the firm was office manager. It was obvious what he did. He was the primary contact for staff and dealt with enquiries. He was someone that staff could go to regarding equipment and staffing issues.

Mr C was a solicitor, principally dealing with conveyancing, private client and executries. If she had settlements, then Mr C could do the banking for her. The Respondent and Mr B could also do this. TS also thought that the cashier might also have been authorised to deal with the banking when she first started. She said that the Respondent and Mr C had banking software on their computers. All banking transactions took place on those computers. She did not think it was possible to use another computer.

When the witness started work in March 2011, the Respondent showed her the room and computer she was to use. She was not given any initial instructions. The computer was very basic and it had the usual desktop. Legal Aid was set up separately online. She would use her email account on her PC. It was possible to open someone else's email but only on their computer. She could not go on to someone else's computer and log into her own desktop. Each computer had a separate desktop and email. She was not aware of anyone installing their own passwords. The firm was a trusting place. She only sent work emails from her work email account. However, there was nothing to stop her from sending personal emails if she wanted.

If the Respondent was out of his office, she would occasionally work in his room and access his computer. When she switched it on his computer would bring up the desktop and email. The inbox would appear first. She did not do this all the time but it was not unusual for it to happen. The Respondent worked in Lochmaddy once a month on a Tuesday. He generally left the office on Monday returning late on Tuesday or Wednesday morning. These were the main occasions on which she used his computer and generally did it at his request. She cannot think of any specific cases she accessed but it would have been for documents relating to cases. The Respondent knew she accessed his computer. Everyone in the

firm knew that the password was 'letmein'. Her expectation was that anyone could access her PC and find any information they needed. She accessed the Respondent's computer, both on his instruction and on her own initiative. It was suggested to her that the Respondent had earlier given evidence that he had no recollection of her ever using his computer. The witness said that he was mistaken and that was not her recollection.

The witness said that there was no monitoring policy in the office. The organisation she currently works for has a long and detailed information security policy. However, there was nothing like that at Ken MacDonald & Co. There was no understanding that partners' computers were sacrosanct and that staff could not access them. There were no regular staff meetings to discuss office procedures or grievances. The witness said she had never accessed Ken MacDonald's computer but there would be nothing to stop her doing so.

Mr Knight asked the witness about emails which were discovered on 28 May 2013. The witness said that she was aware that a new online banking system was in place and it is her recollection that there was a code required to complete the transactions which had been emailed to the Respondent and Mr C. However, she did not do the banking. Mr B told her that the emails were discovered when trying to sort out a banking transaction.

### **CROSS EXAMINATION OF TS**

The witness confirmed that Mr B was the office manager but said that she had never seen his contract of employment. She disagreed with any suggestion by the Respondent that Mr B did not carry out the duties of office manager.

Mr Burnside suggested that there were two administrators and three users of the online banking system and that Mr B was neither an administrator nor a user. The witness said that she thought Mr B was a user of the system. Her recollection was that he could act as a user if necessary, for example, if the Respondent or Mr C were not around. Mr Burnside suggested that the system used card readers and that the bank would only talk to the Respondent if there was a problem. The witness replied, "*I don't know*". The witness agreed that at times when the Respondent was absent from the office he was contactable by BlackBerry. She could send a message to him and he would respond when he was available. Mr Burnside suggested that on occasion she had left messages for him with the Sheriff Clerk at Lochmaddy. The witness said that she did not remember doing that. However, she did remember contacting him on his own phone.

The witness said that the Respondent was aware she accessed his computer. He had told her that she could do that. There was never an expectation that you could not use someone else's computer. The witness was asked for examples of the Respondent instructing her to go on his computer. The witness said she was unable to give any specific examples but if the Respondent was in Lochmaddy and needed anything he would ask her to do this.

It was suggested to the witness that the Respondent had everything on a pen drive and BlackBerry, but she disagreed. It was not her recollection that the Respondent could access everything remotely. He could get his emails on his BlackBerry but not documents. She had no idea if he had a pen drive or not. She was unable to give any specific examples of the Respondent giving her instruction to use his computer and noted that these events took place six years ago. It was put to her that this did just not happen, however, she said that she disagreed and it did happen. She was not in a position to dispute that the Respondent had a pen drive. However, if he had a pen drive he would still need a computer. The witness repeated on many occasions that the Respondent had asked her to access his computer on various occasions and she had done so. This would always be regarding a client or a case. She disagreed with the suggestion that the Respondent was unaware that she accessed his computer.

Mr Burnside asked the witness about the online banking system. She said it was her understanding that the emails were discovered when Mr B was looking for a code for the online banking. However, she did not do the banking and does not know the reason why Mr B accessed the computer. This is what she had been told by Mr B.

Mr Burnside asked whether there would be any problem with staff sending private emails. The witness said there was no problem with this. Mr Burnside suggested to the witness that she would not expect others to look at her private emails. She said, "*That's the risk you take if others can access your emails*". She confirmed that she was not in habit of reading others' emails.

## **RE-EXAMINATION OF TS**

Mr Knight noted the suggestion that the witness had no permission or instructions to access the Respondent's computer. TS said that this was absolutely not correct. Mr Knight noted that the witness had been asked a number of times why she had accessed the computer. The witness said that she was sorry she could not give any specific examples, but it would most likely relate to documents to do with cases.



The witness said that she became aware of the emails sent by Mr B when he handed them to her, said, "I'm sorry" and left. She did not say anything at that point. Mr B seemed pretty shocked and she was also shocked. How the emails came to be discovered was not her principal concern.

## **EVIDENCE OF MS A**

The witness gave evidence on oath. She is a solicitor and used to work for Ken MacDonald & Co., principally doing matrimonial and civil court work. When she worked for Ken MacDonald & Co. she had her own room and her own computer. Anyone was entitled to use her computer. There was no security. All computers used a universal password 'letmein'. The witness said that the system was "*free for all*" and was "*certainly not Fort Knox*". Everyone used other computers in the office. When she was not in the office, her secretary or the receptionists might check her emails. When on holiday, the witness could check her emails and see if they had been opened up and check that someone was dealing with them.

The witness confirmed that when her computer was opened up using the 'letmein' password, a desktop would appear. Her emails would appear as soon as she logged in. The witness confirmed that she used her work email address for private correspondence. Her architect routinely emailed her at her work because she would see the messages coming in while at her desk. She would also receive receipts for online shopping to her work email. There was no expectation of privacy and "*it was not a big deal*". Everything was quite open. She knew that others could see the emails. There was no formal monitoring policy in place. It was a very small office and very informal. It is not like a big city firm with layers of security. It was normal and expected that people would go on to other's computers for documents and styles. Mr Knight referred the witness to Production 9 in the Complainers' Second Inventory of Productions. This was the information security policy from Ken MacDonald & Co. The witness confirmed that she had seen the document when Mr Knight took a statement from her but she had not been aware of it when employed at Ken MacDonald & Co. She said it covered issues like accounts and the cash room and she did not deal with either of those.

The witness remembered Mr B starting work at the firm. He was effectively the office manager and also did legal work. He carried out a lot of the managerial functions you would expect Ken MacDonald to do. He was authorised to sign cheques and make CHAPS transfers. He recruited and selected personnel. He was a very trusted member of staff and acted as the bridge between the solicitors and other staff. Mr

Knight asked the witness whether Mr B looked after IT. She said an outside agency dealt with IT but Mr B would organise them if required. The witness did not know when the online banking system was installed. If she had to send an online banking payment she would go to the Respondent or Mr C.

The witness said that she had occasion "*all the time*" to use other PCs in the office. Of the 12 or 13 people in the office, she would routinely use six of their computers. However, she would not use the Respondent's. Mr Knight asked whether she ever used Mr MacDonald's computer. The witness said she was not certain there would be anything on Mr MacDonald's computer since he is a "*complete luddite*". There was no prohibition on using the Respondent's computer.

The witness confirmed that TS was the Respondent's trainee and they worked closely together. It was perfectly normal and routine for TS to access the Respondent's computer. There was no difference between the partners' computers and those of the rest of the staff. They were not ringfenced. The culture was that anyone might go onto another computer to look for a style or check emails. It was normal to see people using other computers. There was a universal password. At one point, the witness' secretary, Alison, went on holiday and other staff were not able to get into her computer because she had changed the password to 'letmeinplz'. She did not recall there being any other security on the computers. They were "*very very easy to access*".

The witness said she remembered hearing that the Respondent had pornography on his computer in 2012. It was common knowledge in the office. This was a good six months before the emails were discovered. She remembered being on a Christmas night out and looking at the Respondent and thinking he was not the person she had thought he was. He had always wanted to paint himself as "*whiter than white*".

In May 2013, the witness saw TS crying in her room. She tried to find out what was wrong. She asked Mr B and he said it was personal to TS. At the end of that day, he put over 50 pages of emails on her desk. Mr B told her that he had gone on the Respondent's computer to deal with a banking issue. The Respondent had been in Lochmaddy Sheriff Court that day. She thought that something must have been required from a particular computer. She did not know the specifics.

#### **CROSS EXAMINATION OF MS A**

Mr Burnside queried the witness's use of the word 'entitled'. The witness explained that it was a small office. Its objective was to run properly. In the absence of someone, you did what needed to be done. She said a secretary might go on to her computer for a style disposition or a style discharge for a

particular bank. The witness was asked whether she ever used the Respondent's computer. She said she was employed by the firm for 12 years and cannot say she was never on his computer. It is possible. His computer was never ringfenced. If she had done so, she would have had a reason to do so. The witness said that for four or five years the Respondent was an assistant with her. Nothing had changed when he was an assistant to when he was a partner or director. She said the fact that he was a partner had no relevance. The work needed to be done one way or another.

Mr Burnside suggested that the Respondent had a BlackBerry and a pen drive and there was no reason for anyone to access his computer. The witness replied that there was every reason to access the computer in the absence of any member of staff. There was no culture whereby the partners' computers should not be accessed.

Mr Burnside noted that the witness had used the expression 'no expectation of privacy' and asked why she had used that term. The witness said this was a well-known phrase in civil and criminal spheres.

With regard to the online banking, the witness said that she did not know whether Mr B was a permitted user. She was aware he signed cheques and authorised BACS and CHAPS transfers. He has a bank device for this. She did not know whether he was a 'administrator' or 'user'. She would go to him if she needed things done.

The witness said she had never seen TS access the Respondent's computer. However, she did recall TS receiving a text from the Respondent regarding her failure to put a court date into his online diary. This suggested that he knew and had instructed her to access his online diary.

Mr Burnside said it appeared that the witness did not have a lot of time for the Respondent and the witness said she did not think many people would. The Respondent is not the person he purports to be.

Mr Burnside said that the Respondent had given evidence on oath that there was no pornography on his computer. The witness remarked that this was strange because Ken MacDonald had told her that the Respondent's computer had to be "cleaned up". The witness made reference to adverts found on the Respondent's computer and the Chair reminded Mr Burnside to be careful the evidence he elicited by his questions.

The witness said that Mr B's role was managerial as well as legal. She did not think there was anything wrong with him printing something off which affected the welfare of the staff.

## RE-EXAMINATION OF MS A

The witness reiterated that she knew at Christmas 2012 that pornography had been found on the Respondent's computer. It was noted that the Respondent denied this. Mr Knight said that either the witness's information was inaccurate or the Respondent lied on oath. The witness said she was sorry to say that the latter might be the case.

A Tribunal member asked the witness if she had asked for the emails. The witness explained that TS had been upset that morning but had not revealed what was wrong. The witness asked Mr B and he "*could not look at her*". He said it was personal to TS. It was an unusual situation. The witness had appointments all day and then Mr B dumped the emails on her desk just before 5pm. The witness was not aware of Mr B showing anyone else the emails. On Friday he gave them to Ken MacDonald, the other director. She said it was "*such an odd situation*". Mr B "*looked so solemn*". She did not recall any conversation with him at that time but she did speak to him about it subsequently.

The same member asked if the witness had asked Mr B how he came by these emails. The witness said she did not remember. She remained in the firm for three years after this incident and it was still the talk of the place when she left in March 2016. She had been party to countless conversations about it. She did not recall the specific conversations with Mr B. The witness knew about the emails before Ken MacDonald. Mr B had been "*hugely vexed*". He knew he had to do something about it. He knew TS was suffering during her traineeship. He took a risk as an unqualified member of staff to bring this to Ken MacDonald. The Respondent was going to be the successor to the firm and if he was to leave this would really affect Ken Macdonald's retirement plans. The witness said she believed Mr B had given her the emails so she could understand why TS was feeling upset.

## EVIDENCE OF MR B

The witness gave evidence on oath. He still works for Ken MacDonald & Co. He started work there on 11 June 2007. His role is "*office manager and legal assistant*".

He was referred to his contract of employment which was Production 1 in the Second Inventory of Productions for the Complainers. He indicated that his signature was present on page 4 and dated 1 April 2009. He said that the contracts were "*slow in coming through*". They were drawn up from a template but he did not know who did that. He was asked why the contract was dated the same date as the

Respondent was assumed as partner. He said perhaps Ken MacDonald was "*tidying things up*". The witness was referred to Production 2 in the Second Inventory of Productions for the Complainers, a letter addressed to him from his employer. He indicated that the signatures belonged to the Respondent, Ken MacDonald and himself.

The witness reiterated that he was the office manager. His duties were pretty varied. He would change the lightbulbs, deal with office supplies, make sure the staff were happy. It was a small office and lots of people were working there. There were lots of small issues to deal with without bothering the directors. If, for example, new computers were to be installed, the witness would measure the rooms. If staff were to move rooms, he would arrange this. He would ensure that photocopiers and supplies and equipment were in working order. His role with regard to IT was to ensure everything was in working order. He would call in an outside agency when required. He would fix what he could.

The witness was informed that the Respondent had given evidence that the witness was not the office manager in May 2013. The witness said that he was the office manager when he started and certainly after he got the contract.

The witness explained that in May 2013 some staff had passwords to access their computers but all were kept centrally. Most staff did not have a password. Their computers could be accessed in their absence and it was normal for this to happen. The witness had his own office and PC. There was no password on his PC. It was suggested to him that the generic password may have been 'letmein'. The witness said this might have been the case. The witness explained that on opening the computer, his email inbox would appear. This was the same for everyone. If someone was on holiday, very often their computer would be switched on every day and their emails checked.

The witness was referred to Production 9 in the Second Inventory of Productions for the Complainers which was the firm's information security policy. The witness said this was composed around the time the firm changed its online banking system because the bank had insisted on the firm having a policy. The witness was told that the Respondent and Ms A said they had never seen it before. The witness said the only signed copy he had been able to find was signed by Mr C in October 2013. The witness said he thought that after the Respondent left, the policy was altered. It was noted in the document that the principal of the firm was Ken MacDonald so the Respondent had probably left by then. The witness was asked prior to the inception of this policy, what the staff knew about information security. The witness said emails were not for personal use but this was not strictly enforced. He was aware that holiday

confirmations etc. would come into the office emails. When everyone started work, they would be told about confidentiality and emails.

The witness was referred to Production 3 in the Second Inventory of Productions for the Complainers, an application for online banking. The witness explained that the firm used online banking but was moving to 'Corporate Online'. It was the Respondent and Mr C who operated the firm's online banking and practice. The witness was not involved at that time. A number of the staff had fobs to allow them to set up payments but authorisation had to come from the Respondent or Mr C. Mr B would set up payment by accessing Corporate Online. The fob would give him a security number and once it was set up Mr C or the Respondent would go on to their own system and sign it off. They had a keypad and a card to do this. The cashier had a fob but the final authority came from the Respondent or Mr C. Mr B is responsible now for online banking payments.

Prior to Christmas 2012, Mr B found two files which contained pornographic images on the Respondent's desktop. When he came back to work after New Year, he told the Respondent it was good practice to keep "*private and confidential material*" in a safer place. He told him that their IT provider could access the material when upgrading the system. They worked in a small place. If these images were found it would be spread around. The witness said he did not speak to anyone else about finding it, only the Respondent. He did not reference pornography specifically, just said "*anything private and confidential*". Mr B said that on this occasion he had been on the Respondent's computer to print off a disposition which had been emailed to the Respondent. He did not need the Respondent's permission to access this email. However, the Respondent did not know he was doing this because he was not in the office.

Turning to events of May 2013, Mr B explained that Mr C experienced problems making an online payment. This was not unusual. The system was new and there had been a few glitches. The Respondent had originally dealt with Corporate Online for assistance. The payment was for Ken MacDonald. Mr B did not know if he was asked or whether he volunteered to look for information from the Bank of Scotland on the Respondent's computer. He was looking for any email regarding a resolution to the recent similar problems. The staff had made 'dummy payments' before in order to become more familiar with the system. Before going on to his computer, the witness did not think about calling the Respondent in Lochmaddy. He was in court. The witness thought he would try to resolve the issue first. He did not think that the Respondent would be able to resolve the problem on the phone.

The witness could not remember if the computer was on or not. The inbox popped up and he scrolled down looking for a name. He was looking for a female name from the Bank of Scotland. Another name came up. He did not think any other female names appeared before that one. There were not a lot of emails but he would have recognised the names because they generally dealt with the same firms all the time.

The witness was referred to Production 8/2 of the Second Inventory of Productions for the Complainers. He confirmed this was the first email he found. After he had seen that email he kept looking for the Bank of Scotland email. He found what he was looking for in an email containing general guidance about payments which informed him that everything had to be signed off twice, not once. This was general advice contained in an email which had come from a female at the bank. He took that information to Mr C and made the payments. He returned to the Respondent's computer and searched for the name in the search box which he had seen earlier. He printed off a number of emails using the printer in the room. He was pretty sure he then closed the emails and shut down the computer but could not remember for certain. He said it took about five minutes from putting the name into the search box to leaving the office. It probably also took about five minutes to find the banking email.

The witness said he did not need the Respondent's direct permission to go on the computer because this was something that could happen at any time. For example, the property manager, or the trainee would use the Respondent's computer. There was no unwritten rule that partners' computers were private. The witness was aware that the Respondent had a BlackBerry. He was not sure whether the Respondent stored work on a pen drive. He would not be surprised if he did.

The witness said that he spoke to TS about the emails and gave her copies of them. He did not speak to Ms A at that time. He could not remember whether he had given copy emails to Ms A but may have done so. The witness confirmed that it was not until Friday that Ken MacDonald was informed. He went to speak to TS and she said that she did not want anything done because she was afraid she would have to leave the firm. The witness said that he was not worried about his own position. He did not think he did anything wrong in accessing the computer. He did not breach any guideline in the firm. He could not recall whether he accessed the Respondent's computer on any other occasion. He only remembered these particular incidents. When he went on the computer in May, the material he found in December was still there. It was not deleted or password protected. Mr Knight noted that the Respondent gave evidence that there was no pornography on his computer in December 2012. He asked Mr B whether the Respondent is lying about this and the witness said "yes".

**CROSS EXAMINATION OF MR B**

The witness was asked whether he accepted that the information security policy was not in force in May 2013. The witness agreed that the only dated policy post-dates the Respondent leaving the firm. Mr Burnside asked whether the policy was in force or circulated or promulgated in May 2013. The witness said he did not know whether it was circulated to staff. He did not see it then.

The witness could not remember if the Respondent worked long hours. The witness agreed that there would be little or no requirement for people to use the Respondent's computer if he was present. The witness agreed that he worked mainly for Ken MacDonald in terms of legal work. He had no reason to access the Respondent's computer on a regular basis. Mr Burnside said that the witness had heard about the Respondent's position regarding the BlackBerry and pen drive and asked whether he agreed that. The witness said "*probably, depending on the circumstances*".

The witness explained that in December 2012, a draft disposition was engrossed and emailed to the firm. Someone came into the firm to sign it and it was not available. They found out from the other firm that it had been recently emailed. The witness went looking for the document in the Respondent's emails on his computer. He came across a number of files with female names and opened two of them. There was no particular reason to open them. They were on the desktop. Mr Burnside confirmed that when the witness turned on the computer, the image came up and the witness said yes. The witness did not confront the Respondent with this allegation. He might have told Ms A about it later but not at the time. Mr Burnside noted that Ms A had said she knew about it at the Christmas party and the witness said he had trusted her and confided in her. Mr Burnside asked why the witness did not say to the Respondent, "*I found pornography, you should delete it*". The witness said that he found it embarrassing to raise the topic. He agreed that if he had told the Respondent then it would have been foolish to retain it. Mr Burnside suggested to the witness that he did not have any conversation with the Respondent about this. The witness disagreed and said he did not refer to it specifically but if someone had said to him that private and confidential material had been seen on his computer, he would have removed it.

The witness was asked again about the banking problem in May 2013. He said that Mr C had authorised and signed off payments but they were not coming out of the firm's bank account. The Respondent had experienced similar problems and had received guidance from the bank. The witness could not speak to the bank directly because he was not an authorised user. The witness agreed that he could have contacted the Respondent at Lochmaddy. However, instead he looked at the Respondent's computer. He said that he was curious to see if the image was still there. The pornography was still present. Mr Burnside asked



the witness why he did not search for "Bank of Scotland" and the witness said that he did not know. It was a "*rushed thing*". Although it sounds sensible now to search, he was in a hurry. The witness was not having a look at the Respondent's personal emails. It was his office email. In his wildest dreams, he would not have expected to find that material on the Respondent's work computer.

It was suggested to the witness that he was on a "trawl". Mr Knight objected to this question as there was no relevant averment on the Record and the matter was not put to the Respondent. The Chair upheld this objection. The witness was asked to offer an explanation for why he was on the Respondent's computer and he reiterated that he was looking for the Bank of Scotland email. Mr Burnside suggested that the emails were of a private and personal nature. The witness said that he did not accept that private and personal emails exist on a work email system. Mr Burnside asked whether the witness was saying he was entitled to read any emails just because they had the firm footer on them. The witness said they were on the office system and from an office email address. The content was obviously not firm business.

Mr Burnside noted that the witness did not go to the Respondent or Ken MacDonald but took the emails to another member of staff. He was asked whether this was appropriate. Mr B said that it was appropriate in the context of what was going on in the firm at the time. The witness did not go to Ken MacDonald immediately because he knew TS's position on other matters. He knew she was afraid for her job. He showed the emails to her. He did not remember discussing the issue with Ms A but he did certainly discuss it with TS. The witness reiterated that it only took five minutes to locate 50 pages of emails. He said the printing took longer than the finding. The witness said he was not familiar with codes of practice regarding looking at other people's emails.

## **RE EXAMINATION OF MR B**

The witness said when he went into the Respondent's room, in his mind he was looking for any advice on the process of making an online payment rather than anything specific. He agreed that he probably should have searched for "Corporate Online" rather than looking for a female name. However, the Respondent had told him he was dealing with a woman at the bank. He did find a help tool. It did not require an administrator's input to make it work.

A Tribunal member asked the witness whether he was quite sure that it was Production 8/2 in the Second Inventory of Productions for the Complainers which the witness had first come across. The witness said he was "*quite sure it was this one*". The witness agreed that the date on the email was January 2012. He said the advice from the bank when they were having previous problems was probably received early

2013. The member asked the witness how it was that the email from January 2012 was found and the witness said he was scrolling through. He was not sure why this one came up.

A Tribunal member asked the witness about the IT security policy. The witness did not know when this had come into force. He said that the staff were aware of the principles in it.

It was confirmed that the witness was not a solicitor.

### **SUBMISSIONS FOR THE RESPONDENT**

Mr Burnside referred to his written submissions which he had lodged with the Tribunal. They were as follows:

“As directed by the Tribunal, what follows is a written submission on behalf of the Respondent. References is made to the previous Note of Argument for the Respondent, which is to be considered as incorporated in this Note.

The Respondent gave evidence first. He faced a difficult situation in so doing. Although it was not the function of the Tribunal on 26th April 2019 to consider the content of the emails, it was obviously embarrassing for the Respondent to be aware that, of necessity, the members of the Tribunal would have read what were intended to be deeply personal messages to an intimate friend.

Having regard to that fact, I would submit that he gave his evidence remarkably well.

He was, at the relevant time, a co owner of the business and, although the witnesses for the Complainers hastened to advise us in response to questions from Mr Knight that the email accounts of the owners were not sacrosanct, the Respondent reasonably believed that junior employees would not access his computer, particularly if the Tribunal accept his evidence that there was no need so to do.

There may well have been the ‘open house’ situation described by the witnesses for the Complainers in terms of the lack of password protection within the firm but, as a matter of practicality, the Respondent’s method of working did not require anyone else to access his computer.

The Respondent testified that he was always contactable in the event of information being required and he had not given any other person permission to access. He appeared to be genuinely surprised that TS claims to have accessed his computer on a number of occasions. Ms A testified that she had never had occasion to access and Mr B, who did not work for the Respondent, had no need so to do.

We spent some time on 26th April discussing the employment situation of Mr B. The Respondent's evidence was that he never seen the contract of employment for Mr B until it was lodged as a production by the Complainers. His signature on the later amendment, following the incorporation of the business, did not require him to read the original and he testified that he did not do so.

Although, as I have said, we spent some time discussing the status of Mr B, it was perhaps not greatly significant other than enabling him to claim some degree of authority which had not been given to him, irrespective of his title.

The primary point remains that the Respondent had legitimately a reasonable expectation of privacy in terms of his ECHR rights.

In looking at the evidence led on behalf of the Complainers, it is appropriate to start with Mr B. I would suggest that his evidence be scrutinised with great care. Mr B, in my submission, would have been well aware that he was acting inappropriately, despite the 'soft ball' question put to him at the end of his evidence to which he replied that 'he had done nothing wrong'.

There was also the 'red herring' relating to a policy about which he was extremely vague and had never been seen by the Respondent or the other witnesses from the Complainers. It appears to have been signed in October 2013 which was after the Respondent had left the firm. Mr B stated that 'prior to the policy, emails were not to be used for personal matters'. There is simply no basis for that assertion and it is another attempt by Mr B to justify his conduct.

In respect of the first instance of access, Mr B claimed to have been looking for a conveyancing document because the Respondent was 'absent from the office'. The Respondent gave evidence that he was not absent from the office at that time because of his involvement in a major matter, and that his only absence would have been a short one at court, where he would have been easily contactable.

Mr B claimed that while looking for the conveyancing document, he saw a folder with a female's name. He claims to have opened it and found it to contain pornographic material. Quite why he would open a folder which was not connected to the alleged purpose of his search was not made clear.

In the amended complaint, it was stated in paragraph 2.3 that Mr B, having found the alleged pornographic material, 'advised the Respondent on his return to the office that he should delete the said folder....'. There is an inherent unlikelihood of such a scenario being accurate and truthful. Although it must obviously be speculation about the situation, the reaction of the Respondent, one might imagine, would be either to react angrily about the intrusive action of Mr B or to remove the offending

material to assert that the Respondent did neither is simply not credible. I would ask the Tribunal to accept the Respondent's evidence that there was no such material and that no such conversation took place. Perhaps realising that such a scenario lacked credibility, Mr B, in his evidence in chief, departed from the wording in the original complaint (which presumably had arisen out of information provided by him to the Complainers' solicitor) by stating that 'in the new year, he had mentioned to the Respondent that private and confidential material should be kept in a safe place'. That amended version of evidence is also denied.

The second episode again lacks credibility. On this occasion, the claim by Mr B was that he was looking for details of an online banking payment. According to the Respondent, no such detail would be on his computer as the bank do not correspond by email in that respect. Be that as it may, Mr B claimed that in order to seek the information, he decided not to search under the heading 'Bank of Scotland' but to search for a female's name as he believed that the email, for which he was searching, had come from a female.

Members of the Tribunal may recall that I repeatedly questioned Mr B as to why, if he were genuinely looking for a communication from the bank, he would not use the bank's name as a starting point but no satisfactory response was received.

Mr B then stated that he saw an email bearing a female's name (Complainers' Production 8/2) dated 18th January 2012, a date some sixteen months prior to the date of his search. The Respondent gave evidence that to the best of his recollection, he received about 500 emails per month and in order to go through the sixteen month period concerned, some 8,000 would have been accessed. The terms of email 8/2 were clearly personal and had nothing to do with the firm's business. Mr B then claimed to have found the bank information but not satisfied with that, he returned to the Respondent's office to search for any other correspondence from 'Ms D' who had sent the email of 18th December 2012 and went all the way back to April 2011, a further nine month period, involving a further 4,500 emails.

At that point his excuse that he was carrying out a lawful function of his employment is completely discredited. He is clearly 'trawling' for personal information relating to his employer. He prints off the personal emails of his employer, but does not go to the Respondent or Mr MacDonald, co owner of the business. If he had felt that he had any degree of entitlement to do what he had done, then such a course of action would have been more appropriate.

Instead, he provided a copy of the email trail to TS, the trainee solicitor, on the basis that she was referred to in the exchange. He also states that he 'may have given a copy to [Ms A]. It is odd that he uses the word 'may', given the evidence of [Ms A] that he provided her with an unauthorised copy of the emails. This is perhaps in an attempt to appear more reasonable.

It is perhaps appropriate for me to make reference to the two further witnesses led for the Complainers, Ms A and TS before moving on to the legal arguments.

TS was clearly unhappy with the Respondent and I do not criticise her for that. She was in the unfortunate position of reading comments about herself which it was never the intention of either of the parties, in a private email exchange, to reveal to her.

Ms A was with, perhaps less justification, hostile to the Respondent. I noted early in her evidence that she stated that 'anyone was **entitled** (emphasis added) to access the computer of anyone in the office'. She talked about 'a free for all'. Unlike Mr B she did indicate that persons using the computer system could send private as well as business messages. She then used, unprompted, the phrase that there was 'no expectation of privacy' which of course, forms the basis of the ECHR argument and, in my view, was clearly designed to anticipate the Respondent's case. She did, however, confirm that she had never seen Production 9, the policy document.

Having reviewed the evidence I now turn to look at the legal issues. Article 8 of the ECHR provides the right to respect for private and family life and states:

- '1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There should be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.'

The SSDT is a public authority under section 6(3)(a) of the Human Rights Act 1998. Mr Knight has in his written submissions and questions to the Respondent, at the April hearing, made much of the fact that an ECHR point was not taken at an earlier stage. Be that as it may, such an omission, if it is one, is irrelevant. What the Tribunal have to decide is whether or not **they** would be breaching the Respondent's Article 8 rights by considering the Respondent's private correspondence. In my view, it does not matter that the correspondence has been seen by the Law Society and Scottish Legal Aid Board. The outcome of this case could have extremely serious ramifications for the Respondent's career and this forum is the appropriate place for the plea to be made.

I made reference to the important case of *Barbulescu v Romania*. It is a very lengthy judgement and I have been asked to refer the Tribunal to the most relevant parts.

Because Barbulescu had been employed by a private company, the monitoring of his communications and his ultimate dismissal for breaching the company's IT policy, could not be regarded as interference with his rights by the State. However, the employer's actions were effectively sanctioned by the domestic employment courts (Emanations of the State) when they rejected his claim. In these circumstances the European Court of Human Rights found that the Complaint should be examined from the stand point of the State's positive obligations.

I direct the Tribunal to paragraphs 121 and 122 of the Judgement which sets out the factors which the domestic authorities should treat as relevant.

The Respondent had not been 'notified' that his correspondence would be monitored. Despite the suggestion that there was open access on some sort of 'free for all' basis, the Respondent's clear evidence was that his method of working did not require anyone else to access his account and to the best of his knowledge and belief, no one did so. Subsection (vi) of paragraph 121 states that 'there should be safeguards to ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality'.

In paragraph 141 of the Barbulescu judgement, the court reaches its conclusion.

In my earlier note of argument, I deal with the type of correspondence protected by Article 8 and I do not propose to repeat what I have said. The justification relating to the protection of the rights and freedoms of others does not, in my view, apply for the reasons I have set out in my original note.

I now turn to the Information Commissioner's Office Employment Practices Code. Part 3 of the Code provides guidance on monitoring at work. There is no definitive definition of 'monitoring'. However, the Code provides a number of examples to which the code applies, including 'randomly opening up individual workers' emails or listening to their voice mails to look for evidence of malpractice'. Although Mr B was not systematically monitoring the Respondent's emails, there is no doubt that he was randomly opening up a large number of the Respondent's emails which he had no right to do. In my submission, there is clear evidence of a breach.

Page 58 of the Code refers to the adverse impact which monitoring may have on workers and refers in particular to an intrusion into their private lives.

Page 59 of the Code provides examples of monitoring and Page 61 states 'bear in mind that the private lives of workers can, and usually will, extend into the workplace'. The same pages refer also to the relationship of mutual trust and confidence that should exist between workers and their employer.

Page 63 of the Code deals with the fact that any intrusion should be no more than absolutely necessary and that a significant intrusion into the private lives of individuals would not normally be justified unless the employer's business is at real risk of serious damage.

No consent as envisaged at the foot of page 63 was given by the Respondent and no consent has been obtained from the other party to the communications,

Pages 65 to 73 give helpful guidance to employers regarding the monitoring of electronic communications to which the Tribunal's attention is respectfully directed.

A very important point is made in page 70 relating to making the contents of a communication available to a third party.

Finally in respect of the Code, the Tribunal's attention is directed to page 72, paragraph 3.2.8 which states 'wherever possible, avoid opening emails, especially ones that clearly show that they are private or personal'. The following 'key point' states 'ensure that email monitoring is confined to address\heading unless it is essential for a valid and defined reason to examine content'.

The last authority which I have lodged is the Guide on Article 8, produced by the European Court of Human Rights (updated on 30th April 2018). Again this is a lengthy document and I shall draw the Tribunal's attention only to certain paragraphs.

The first of these paragraphs is 116 which refers to the *Barbulescu* case and reiterates the relevant factors.

Paragraph 388 gives further information in support of the right to respect for correspondence, with paragraph 389 indicating that 'new technologies' are included within the scope of Article 8.

Paragraph 393 deals with screening of correspondence and making copies and forwarding of mail to a third party. It is accepted that these acts were not carried out by public authorities but it is submitted that consideration of information obtained in breach of the principles of Article 8, would be a contravention of the Respondent's rights.

Paragraph 395 deals with the State's positive obligation when it comes to communications of a non professional nature in the work place (*Barbulescu*) and an obligation to prevent disclosure into the public domain of private conversations. I anticipate that Mr Knight may argue that there has already been disclosure by reference to the fact that the emails have been seen by the Law Society and Scottish

Legal Aid Board but, that said, there remains the obligation on the part of this Tribunal not to make further disclosure.

Paragraph 397 reminds us that 'an interference can only be justified if the conditions set out in the second paragraph of Article 8 are satisfied. Thus, if it is not to contravene Article 8, the interference must be "in accordance with the law", pursue one or more "legitimate aims" and be "necessary in a democratic society" in order to achieve them'.

It is accepted that this case does not involve a regular system of monitoring as such but, the employee's right to protection is not, in my submission, dependent upon there being a regular system. What Mr B carried out was an unauthorised and unnecessary search of the private correspondence of his superior. He has improperly copied that correspondence and provided it to third parties. It must have been obvious to him that the correspondence was of a private and personal nature and that he did not have the consent of either party to that correspondence to read the correspondence, far less to make it available to other people.

There is an important principle at stake here and, in my view, the Tribunal must clearly uphold the Respondent's Article 8 rights and not allow the email exchange to form part of the Complaint against him."

Mr Burnside also addressed the Tribunal on the written submissions for the Complainers. He suggested that the motion for expenses was unusual at this stage of proceedings and was intimidatory. He said that the Answers he lodged were confined to the emails because that was the fundamental point which required debate. A debate was fixed but it became clear that the Complainers were not prepared to accept a debate on the pleadings and it was the Fiscal's view that the Respondent should lead evidence. Mr Burnside acceded to that but it was not his choice. He said the reference to "abortive proceedings" was an inappropriate description. The Respondent understands that if he is ultimately unsuccessful, he will be liable in expenses.

Mr Burnside said that he had asked the Fiscal for precognitions and Mr B's contract of employment. The Fiscal was not obliged to provide these and had declined. Mr Burnside had therefore been "in the dark" to an extent regarding the evidence to be led. He accepted that it was the Respondent's plea and he therefore ought to go first. However, he was disadvantaged because he did not know what points were going to be made later. In hindsight had he known the extensive evidence that would be led for the Complainers, he would have suggested a two-day hearing. A lack of time meant certain matters were not put to the witnesses by him in cross-examination.



Mr Burnside noted that a Tribunal operates differently from the Court of Session. The Record should not be examined line by line. The Respondent had a duty to give an explanation in his Answers. The Record set out his position which was that he had a reasonable expectation of privacy. A Tribunal need only act fairly.

He said that the reasonableness of the expectation of privacy must be construed by reference to the individual solicitor and not the other people in the firm. He drew an analogy with employment law. A suitable offer of employment is to be construed from the point of view of the individual concerned. Mr Burnside submitted that the Respondent had a reasonable expectation of privacy. His method of working meant that no one else required to access his computer. If he genuinely believed anyone could access his computer, he would not have retained the emails. It supports his belief that he thought they were private. "Rightly or wrongly" he had a reasonable expectation of privacy.

Mr Burnside noted that the Fiscal referred in his written submissions to a lack of candour on the part of the Respondent. It must have been difficult and embarrassing for the Respondent to give evidence. He had always intended the material to be personal and private. He submitted that the Respondent's position on Mr B's employment title was genuine. His view is not disproved by his signing the docquet. He did not read it and all employees got the same docquet. It does not prove he ever saw Mr B's contract of employment. It would be a dangerous leap to say that the Respondent was not credible. He accepted there were no physical constraints preventing access to his computer. However, the governing feature was his reasonable belief in his privacy. Mr Burnside noted that the pornography issue never appeared in the original Complaint but was added by amendment. He can only think it was added in an attempt to discredit the Respondent. Mr B in his evidence departed from the averments in the Complaint with regard to the alleged conversation with the Respondent, "presumably because he realised he went too far". If Mr B is truthful about the alleged conversation, the Respondent would have removed the material or challenged his access. This suggests that the conversation never took place. Mr B's explanation lacks credibility.

Mr Burnside highlighted the different internet banking roles of user and administrator. He noted that only Ken MacDonald and the Respondent were administrators. He suggested that the reference to an information security policy was a "red herring". The only one produced was dated October 2013, after the Respondent had left the firm.

He asked the Tribunal to think about the reason why Mr B had not searched for 'Bank of Scotland' and why he claimed to be looking for a female name. The Respondent does not know why Mr B accessed his emails. Mr Burnside was therefore unable to put a contrary explanation to the witness when his explanation "beggars belief". Mr Burnside submitted that the exercise was a trawl and constituted a gross invasion of privacy.

He noted that Ms A was keen to talk of "entitlement" to access and a "reasonable expectation of privacy". These witness had been freshly precognosed about things which happened six or seven years ago. They had been properly advised of the issues and the defence. Ms A allowed her sympathy for TS to slant her evidence.

Mr Burnside said his client does not know why Mr B misrepresented his position as office manager. However, he submitted that it was not important because it was his actions which were inappropriate. Would Mr B have stopped even if the emails had been marked 'private'?

Mr Burnside asked the Tribunal to look at the terms of the first plea-in-law and noted that it referred to the emails being obtained without authority or the knowledge and consent of either party. This was never attacked. No consent was sought from either correspondent.

Mr Burnside said he accepted that there are authorities relating to admissibility of evidence but they can all be distinguished. Craven related to a work matter sent to a fellow employee. It related to an essential part of the firm's business. The same comment could be made about West. In Henderson & Marnoch, the police recovered information in good faith. Mr B was not acting in good faith when he accessed the information and provided it to a third party. The Respondent's position was that the business operated on trust. As an owner, he genuinely thought because there was no business need he did not have to be concerned about people accessing his emails. Ratray involved a divorce action and could be distinguished because the letter was given to a third party. He could not see the relevance of Pringle to the present situation.

Mr Burnside said he accepted the circumstances did not constitute formal monitoring. However, random access can constitute monitoring. Mr B accessed and trawled through the emails of his employer and director of the company without the consent of either party and passed on the material to a third party.

Mr Burnside claimed it was not relevant that the privacy argument had not been made before any other body. The important body for the Respondent was the Tribunal. It can have a defining effect on his

career. The fact the emails have been in the possession of two other bodies does not mean that the Tribunal is not bound by Article 8. The Respondent still has a reasonable expectation of privacy.

Mr Burnside noted that the Fiscal claims that the exceptions to Article 8 apply. However, in the Complaint it is noted that no other parties claim to be directly affected by the conduct. No other party is seeking compensation.

Mr Burnside made reference to Holder, MacPherson and Nawaz. He noted that these involved the rights of a governing body to access accounts information, not personal correspondence. Garamukanwa v UK was authority for the fact that each case turns on its own facts.

In this rather unusual set of circumstances, Mr Burnside submitted that the Article 8 rights of the Respondent were severely damaged and if the Tribunal admits the emails it will be acting in breach of Article 8.

#### **SUBMISSIONS FOR THE COMPLAINERS**

The written submissions for the Complainers were as follows:

“The Respondent has presented a Note of Argument in support of his two preliminary pleas.

He lodged that Note of Argument some time ago, and the Complainers lodged a Note in response, which has now been largely superceded by the Respondent’s amendment. The thrust of the Complainer’s Note in response was firstly that the Respondent’s averments were irrelevant and lacking in specification to support the two pleas and secondly that the factual matrix upon which the two pleas were founded was not admitted nor established.

The Respondent amended his pleadings to seek to address the relevancy and specification issues but it remains the position of the Complainers that there still arise relevancy issues.

It also remains the position of the Complainers that the factual matrix upon which the pleas are founded remains unestablished and in particular after hearing the evidence led at the hearing on 26 April.

For that reason alone the Respondent's position fails.

It is appropriate at this point to comment on the evidence led. It is the Complainer's position in general that there was a lack of credibility and reliability on the part of the Respondent, but also a lack of candour in that averments in his Answers and passages in his Note of Argument were clearly inaccurate on his own evidence.

The Respondent gave evidence that he had not had sight of Mr B's contract of employment. He still maintained that he had not been employed as an Office Manager and this despite the fact that he accepted that he signed updated contract of employment for Mr B dated 26 November 2012 and which is production 2/2 for the Complainers. That element of his evidence had no credibility whatsoever.

He also gave evidence that he had no knowledge of anyone needing to access his computer and he denied that his trainee had been using it with his knowledge or his instruction. We heard evidence from that trainee of the complete opposite and again the Respondent's version of events is not credible.

It was clear from the evidence of the Respondent, and the three other witnesses, that there were no procedures in place and indeed nothing in place at all to prevent access to the Respondent's computer or indeed for access to be taken to anyone else's computer in the firm at the time. The Respondent's position was however that no access was necessary. We have however heard contra evidence to the effect that access to his computer was indeed necessary not only by his trainee but also Mr B to perform some online banking transactions and to seek online banking information.

The Respondent indicated that he treated his email account as both a business and personal inbox. He failed however to give any evidence as to how he had an expectation that that inbox would be private given the circumstances in which there was ready access to his computer and indeed anyone else's computer in the firm's offices.

He denied having any pornography on his desktop and maintained that if Mr B gave evidence regarding that then he was lying. Both Mr B and Ms A gave evidence about. Mr B as the person who found it,

and Ms A who had been informed about it by Mr B. The Tribunal is being asked to hold their evidence as reliable and not that of the Respondent.

The Respondent conceded that both he and the late Mr C carried out online banking transactions. He sought to differentiate between himself and Mr C as being a user but not an administrator. His averments are however disingenuous as he makes a positive averment in Answer 2.3 on page 5 at line 1 that he was "the only person who could have authorised any payment". He also repeats that in the penultimate line of page 1 of his Note of Argument namely "The Respondent was the only person authorised to instruct any online transfers...". His evidence in that regard was completely contradictory.

He gave evidence that there was no security policy in place for the firm despite the fact that he would have been the person responsible for framing such a policy. It never occurred to him to prepare such a policy and he readily conceded that the access to the computers was access to all and that the firm operated on trust.

His evidence was that Mr B was lying about the banking issue which led him to access his computer but nothing was put to Mr B in cross-examination in that respect, no motive or reason for Mr B accessing his computer was put to him in cross-examination nor any contra-position was put to him in cross-examination. Indeed no contra-position is averred by the Respondent in his pleadings as to why Mr B would access his computer on the date in question.

The Respondent was asked a specific question during cross examination about how any other employee in the former firm might know that they could not access his computer. He readily conceded that no one would know that they would need his permission.

It necessary follows therefore that any argument being founded on permission being required cannot be sustained on the basis of the Respondent's own concessionary evidence.

In contrast, the evidence given by TS, Ms A and Mr B was all given in a straightforward and entirely credible manner.

TS confirmed that she was aware that there were two individuals within the firm who operated the firm's online banking those being the Respondent and Mr C. She gave evidence as to the open policy within the office and the use of the "letmein" password if required. She confirmed that there was no expectation within the firm that anyone's computer was private and there was certainly no question of anyone's computer being off limits either.

She gave clear evidence that she had accessed the Respondent's computer on many occasions either on her own initiative to look out documents for cases she was working on or on his instruction for a similar purpose. She also gave evidence that Mr B would on occasion operate the online banking facility if the Respondent and Mr C were both absent from the office. This would necessitate him accessing either Mr C or Mr Macpherson's computer.

She also gave evidence that as far as she was concerned the Respondent would know that others and in particular herself were accessing his computer when he was out of the office. She again reiterated that she had on many occasions been instructed by the Respondent to access his computer and carry out work which he was wishing her to undertake. Her evidence in that regard was not tested in cross-examination. There is no reason to disbelieve TS's evidence in this regard and again it all points to there being no question of permission being required to access the Respondent's computer.

Ms A confirmed that Mr B was the Office Manager in the firm and that from her standpoint he ran the office. Quite why the Respondent would still question whether Mr B was not the Office Manager in his own evidence remains an issue which the Respondent has manifestly failed to address.

She likewise confirmed that as far as access to other computers was concerned in simple terms anyone could go on to anyone else's computer and access their desktop. There were no restrictions. She herself had no expectation of any privacy in respect of the computer that she operated and she knew that her emails might be read either by her secretary or indeed by anyone else who might have to operate her machine. She gave examples of her own private business transactions being easily accessible to others and she was aware of that and took no exception to it.

She also gave evidence that she became aware of the pornography being found on the Respondent's computer, and that he had been told to delete it but she could not recall precisely when that date was.

When it was put to her that there might be some different level of access applicable to the Respondent's computer because he was a Partner/Director, she rejected that contention and maintained that there was no question of the Respondent's computer being ring-fenced for access purposes.

It may be suggested that Ms A's evidence was in some way tainted by her view of the Respondent. The Respondent really only has himself to blame for that. She was asked a direct question in cross-examination about her view of the Respondent. Given the material which is before the Tribunal, it is hardly surprising that a female colleague of the trainee solicitor in question has taken a dim view of the Respondent's character. That should not impact on her credibility.

Mr B gave the evidence about his appointment as Office Manager and referred to his contractual documentation. Again the Respondent's position on that has to be referred to. Why would Mr B misrepresent the position regarding a position of employment which he has held since 2007 and which was confirmed in writing by the Respondent himself ?

He gave evidence about his duties within the firm back at the material time and also the present date and gave evidence about the IT system in operation within the firm. He confirmed, as all the witnesses did, that there were no access restrictions on the computers within the office. Certain people had their own computers on which their own mail inboxes were loaded but these were not password protected and in the event of anyone else requiring to access a computer people would know that the desktop would open and that person's mail inbox would be there.

Perhaps of some significance he indicated that he was surprised that if the Respondent felt that he was entering into private or personal correspondence on non-firm's business, he would have expected such correspondence to be marked appropriately. As the evidence has shown, there were no such markings and it was readily accessible to anyone who looked at the Respondent's computer and his mail inbox.

He referred to the security policy which he had managed to locate and he was unable to precisely state when this policy may have been in force. He indicated that it had been framed at the request of the firm's bankers but it transpired that the Respondent had had no involvement in that. This of course was contrary to the Respondent's evidence in which he maintained that if such a policy were required

by the Bank he would have been the person responsible for framing it. Again the Respondent's evidence was contradicted and shows a lack of credibility on his part.

Mr B gave evidence about the online banking facilities and who were authorised users.

More particularly he gave evidence regarding the events in May 2013 and how he came to be accessing the Respondent's computer on that date. Whilst it was put to him that he had no right or permission to do so, no question was posed of him in cross-examination as to why he had no such right or permission. It might perhaps be implied from the Respondents position that Mr B had carried out a trawl of the Respondent's emails but nothing was put to him on behalf of the Respondent in that regard. He gave his own evidence as to how he came upon the offending emails in question and there is no reason for this Tribunal not to accept in full the evidence of Mr B in these respects.

He also gave evidence about finding the pornography on the Respondent's computer in December 2012 and also finding it present still on the computer in May 2013 and that despite a warning that it should be removed. Again why would he lie about these issues? He was corroborated to a degree by Ms A and again his evidence should be accepted in full in these respects.

He was also asked the direct question if he has been told by the Respondent or the other Partner in the firm that he needed permission to access either of the Partner or Director's computers and the answer to that was in the negative, and no such permission was required.

In overall terms, therefore, the Complainers would seek to have the Tribunal prefer the evidence of Mr B, Ms A and TS in any respect where it conflicts with the evidence of the Respondent, and to find the Respondent in overall terms to be lacking in credibility and reliability.

There are two pleas in law advanced on behalf of the Respondent:-

1. The emails have been obtained without the authority, the knowledge or consent of the Respondent or other party...had been obtained improperly and should not be admitted to probatation.



2. The use of emails being in breach of Article 8 of the ECHR in respect of the rights of the Respondent and other party, and the Complainers and SSDT being public authorities, should not be admitted to probation.

The averments in support of these pleas are to be found in Answer 3 in the Record. The factual narrative upon which the Respondent founds his position commences on page 4. There remain issues as to whether the Respondent's averments are factually correct and whether he has been able to establish those averments on the basis of his own credible and reliable evidence. This has been commented upon previously and it is maintained that he has manifestly failed to do so.

The averments principally address the second plea and not the first plea. The only averments in support of the first plea are on pages 5 and 6 of the Record and are contained in three separate sentences.

Firstly on page 5, paragraph 2, line 5 "accordingly the said Mr B has no reason to access the computer and did not have the permission of the Respondent."

Secondly in the final paragraph on page 5 at line 2 "no permission had been sought from or obtained from either the Respondent or his friend who had made a number of the comments contained in the email exchanges."

Thirdly in the first paragraph on page 6 at line 3 "said Mr B carried out a detailed and unauthorised search of the Respondent's email account and he misused private communications which he had discovered."

The Respondent has also produced no authority in support of this plea. All the authorities that have been produced are directed towards the Article 8 or second plea.

The primary submission of the Complainers therefore is that there are no averments, no evidence, and no authorities in support of the Respondent's first plea so it falls to be repelled.

In regard to the first plea certain questions arise such as did Mr B have permission to access the Respondent's computer, and whether Mr B needed such permission to access his computer? Whether

he did or not it is now of questionable relevance given that it is clear from the evidence heard that no permission was required in the former firm for anyone to access anyone else's computer and the Respondent conceded in his evidence that no one would know that there might be restricted access to his computer.

The Respondent in order to advance his position has to establish that Mr B had no right of access and required permission. Him saying so is not sufficient, and on the evidence led he has failed to establish his own position.

It also has to be borne in mind that in May 2013 the emails were sent out from a firm email address. That email address and the server upon which the emails were generated and stored belonged to the firm. The Respondent has failed to lead any evidence to establish that those emails were his personal property.

Reference has already been made to the evidence of Mr B, Ms A and TS in respect of the system (or perhaps lack of it) in place and with no one within that firm had any expectation of privacy. Anyone could go on to anyone else's computer and if the emails were left open they could be read by anyone undertaking that access.

Evidence has also been heard, as commented upon, that TS was instructed by the Respondent to access his computer and yet he sought to deny any knowledge of that in his own evidence. That is simply not credible. All of this evidence points to the factual position that no permission was required.

When looking at the issue of permission, there still remains a suggestion from the Respondent that Mr B needed some form of authority to access the Respondent's computer. What he was unable to do however was give evidence himself as to why that authority was necessary. It is averred that Mr B undertook a fishing exercise and monitored the Respondent's emails and that he did not undertake just a cursory look on one particular date. The evidence led does not support the Respondent's position in these respects.

In Answer 3, page 4 line 12 the Respondent positively avers that the position advanced by Mr B was a "false claim". He accused Mr B of being a liar. These are positive and serious averments and allegations, and the evidence that has been heard show them to be without foundation.

Taking all of the evidence as a whole therefore, on the issue of access and permission, there have to be serious reservations about the credibility of the Respondent's position and his own evidence.

The secondary position for the Complainers, therefore, is that there are still no averments and no authorities in support of the first plea but even if that is set aside taking account of the evidence heard and the lack of credibility on the part of the Respondent, and the positive credibility on the part of the other witnesses, there is no basis upon which this Tribunal can consider that this plea is supported by evidence on behalf of the Respondent and it therefore falls to be repelled.

Even if the Tribunal does find favour with the Respondent's position and rejects the primary and secondary positions of the Complainers, taking all of the evidence as a whole, and even giving the Respondent some benefit of the doubt, there is no basis in law put before this Tribunal for refusing to admit to probation the emails on the basis of them having been "improperly obtained".

Authorities numbered 7, 8 and 9 on the Complainer's List of Authorities support the Complainer's position in this respect.

*Ratray –v- Ratray* – reference to the rubric;

*Henderson & Marnoch –v- HMA* – reference to the rubric on pages 1 and 2;

*Baronetcy of Pringle of Stichill* – paras. 1 and 77-79.

Two of those three cases are civil cases, with Henderson being a criminal case, but all deal with whether evidence was improperly obtained and, even if it were, it remained admissible.

It necessarily follows that even if it might be established that Mr B had no right to access the Respondent's computer, (which is of course denied), the fact that he did not have such a right, and found those emails does not of itself render them inadmissible.

Turning to the Respondent's second plea, the averments in support of that are also contained in Answer 2.3.

Firstly in the second paragraph on page 5 at line 6 "in terms of Article 8...the firm did not have a monitoring policy in place."

Secondly in the final paragraph on page 5 and over on to page 6, at line 4 "the Respondent had a right to consider his email account private...the Respondent's right to privacy and contravened his ECHR rights."

Finally in the second paragraph on page 6 "the Respondent believes that such a situation is akin...contravenes the Respondent's Article 8 rights."

When the emails were discovered in May 2013, the firm of solicitors was a limited company and the email and servers containing them were not the private property of the Respondent. They belonged to that firm. The Respondent is only now raising the issue of the reasonable expectation of his privacy. His position in that regard and its lateness again raises questions of his credibility. No challenge was raised to the privacy of these matters when they were investigated by the Procurator Fiscal, the Scottish Children's Reporter's Administration, the Scottish Legal Aid Board, the Scottish Legal Complaints Commission or the Law Society itself during the investigation process. Why is the Respondent seeking to challenge these emails and their content at this late stage ?

Whilst the Complainers do not contend that the Respondent is personally barred from raising these issues at this stage, the level of umbrage now taken has to be considered when no previous challenge was raised. Is this a genuine grievance or is it a poor and somewhat late attempt to have some potentially damaging material removed from this prosecution?

If the Respondent feels so aggrieved at the intrusion of Mr B into his private communications, why would he only raise the issue now? These matters were put to him in cross-examination and he was unable to answer. He was unable to put forward any explanation as to why Mr B might have undertaken the search that he did and if there was any motive for that. He avers nothing in support of an ulterior motive on the part of Mr B.

What is clear is that the firm did not have a monitoring policy. Even if it did, it is questionable as to whether it would be of any relevance. The authorities produced by the Respondent in support of this plea all make reference to monitoring policy cases and more particularly scenarios involving an

employer monitoring an employee. The *Barbulescu* case is just that type of case. The Respondent however led no evidence in support of such a scenario.

We do not have those circumstances in the present matter. The Respondent avers that he was the person responsible if any monitoring policy were to be framed, implemented and put in place. His position is that there was no policy and the evidence would tend to support that. He certainly did not frame one.

This is therefore not a scenario where an employer is monitoring an employee. What we have is an employee with legitimate access, finding emails written by his employer and stored on equipment belonging to the firm.

The Complainer's position therefore is that the authorities founded upon by the Respondent therefore do not apply to the circumstances in this case, even if the Respondent's version of events were given some degree of credibility.

The authorities produced by the Respondent, apart from the Article 8 narrative itself, are therefore of no assistance or guidance to the Tribunal in determining this matter.

Article 8 itself provides (1) that everyone has the right to respect for his private and family life...and correspondence and (2) no interference by a public authority except such as in accordance with law and is necessary...for protection and rights of freedom of others.

On the second paragraph of Article 8 there are no averments put forward on behalf of the Respondent apart from a narrative in the second plea in law itself whereby it is stated that the Complainers and the SSDT are public authorities.

If it is assumed that the Tribunal can consider this matter in the absence of any averments, and if it persuaded that the Complainers and the SSDT fall within the definition of being public authorities, then the Complainers would submit that the exceptions contained in the sub-paragraph clearly apply.

These are legal proceedings concerning allegations of professional misconduct against a solicitor and his alleged improper conduct towards two third parties being his former trainee and employee, and a child witness/client.

Third party rights require to be considered and protected and in the serious circumstances of the allegations here those rights override any rights that the Respondent may have in respect of this sub-paragraph.

The position being advanced by the Respondent is that his private emails were accessed and exhibited to a third party and that he had a right to consider those emails as private. Those are his averments. It is also averred on behalf of the Respondent that an analogy appropriate here is someone looking at personal papers, diary or a telephone. This is an inaccurate analogy because we have evidence that emails were easily accessible, not password protected, stored on a server belonging to the firm, and composed on a firm email address again belonging to that firm.

The Respondent refers to the *Barbulescu* case in support of his position. At paragraph 73 of that authority it is made clear that whilst there can be a reasonable expectation of privacy, that expectation is significant but not necessarily conclusive.

None of the other solicitors or employees within the Respondent's former firm had any expectation of privacy. Even if there were such an expectation, just because that expectation exists does not necessarily mean that if someone breaches that expectation it contravenes Article 8.

Again the Tribunal has to look at the whole circumstances and in particular:-

- Straightforward access to all PC's in the firm.
- No password protection.
- Relaxed/no policy or system in place.
- Respondent in charge of any such policy and nothing formal framed.
- Respondent had a warning in December 2012 regarding inappropriate material on his desktop and failing to heed that warning.
- None of the other employees had any expectation of privacy.

- The Respondent is *prima facie* the employer not an employee so the normal monitoring issues do not arise.
- Lack of any prior challenge on this ground to a number of other public authorities.
- A single accessing of the Respondent's computer by the Office Manager for a legitimate purpose.
- Lastly, and perhaps more particularly, the Respondent's concession that no one in the firm would know that his own PC was somehow off limits.

It is accordingly the Complainers' position that it cannot be sustained that there has been any breach of Article 8 in this case.

The Complainers have produced some authorities in respect of the Article 8 position advanced. In regard to the reasonable expectation of privacy issue authorities 4 and 5 are very similar to the present in that they deal with inappropriate emails and in both of those cases the Article 8 argument was rejected.

*Craven –v- Bar Standards* at paras. 3-4, 31-34 and 39-45;

*SRA –v- West* at paras 16-17 and 34-35.

The sixth authority is again an email case albeit in a matter where there was a monitoring policy. Again the Article 8 argument was rejected but it illustrates that the test to establish an Article 8 breach and get the evidence excluded is an extremely high one.

*Simpkin –v- Berkeley Group* – Extract from Practice Note, page 24, para.3

In respect of the Article 8 (2) position and the exceptions to the rule, the Respondent's Note of Argument appears to accept that the Complainers can rely on that exception but they are not entitled to in the circumstances of this case. Nothing was put forward in evidence as to why the Complainers are not entitled to rely on that exception.

The fact of the matter is that the Complainers are entitled to use the email material to bring this prosecution and protect the rights of the two other third parties being the former trainee and the child client/witness.

The Complainers also maintain that even if the point is reached whereby the Tribunal is still considering whether the exceptions apply and whether a breach of Article 8 may have arisen, and it is suggested that the Tribunal need not get to that stage, there are further authorities which support the use of the exception. Those are authorities 1, 2 and 3 on the list lodged by the Complainers.

*Holder –v- Law Society* at paras 4-5 and 28-35;

*Macpherson v Law Society* at paras 2 and 10; and

*R –v- ICA ex. parte. Nawaz* – at pages 1 and 2 (rubric).

In summary, therefore, the Complainers would invite the Tribunal to repel both of the Respondent's preliminary pleas and send the Complaint in its entirety for a full hearing.

Given that the Respondent has not provided a full set of Answers to the Complaint as yet, the Complainers would suggest allowing the Respondent a further three weeks to provide final adjustments to his Answers with the Complainers being given three weeks to adjust in response.

Lastly, the Complainers seek the expenses of this process to date given that the procedure thus far has been undertaken in respect of the Respondent's preliminary pleas, Notes of Argument, Preliminary Hearings and response to the preliminary position advanced by the Respondent. There was also an abortive previous Preliminary Hearing as the Respondent then determined that he wished to lead evidence in support of his position.

The Fiscal also addressed the Tribunal. He said he had laid out the evidence. He suggested that the Respondent was not credible and reliable and had displayed a lack of candour. However, this was a "jury question" and was for the Tribunal to determine.

The Fiscal noted that if a Respondent advances a preliminary issue and produces a note of argument and the averments are disputed then he must establish the facts. The Fiscal's position was that the Respondent had not established his position. This did not preclude the Tribunal from applying the law to the facts found by the Tribunal. The Tribunal ought to find the facts and then establish if they constitute a breach of Article 8.



The Fiscal noted that seldom does one find a case on all fours with a present case. Considerable work had been undertaken by the Complainers to find cases which supported and undermined their own case. No cases were found which support the legal position advanced by the Respondent even on the facts advanced by him. He summarised the cases upon which the Complainers relied. He submitted that Barbulescu was not supportive of the Respondent's position. In that case an employer was monitoring an employee. In the present case an employee with legitimate access had "stumbled upon" the material.

## DECISION

The Respondent sought to exclude several emails from probation. Firstly, he said this should be done on the basis that the emails had been obtained improperly without either correspondents' authority, knowledge or consent. Secondly, he argued for their exclusion on the basis that the use of the emails in Tribunal proceedings would infringe the correspondents' Article 8 rights.

Based on the oral evidence, the Tribunal established the factual position set out at paragraphs 11.1-11.3 above. This was not without difficulty. The Tribunal did not consider the Respondent to be a credible or reliable witness. His evidence, for example regarding Mr B's role as office manager and TS's permission to access his computer, lacked credibility. Ms A's testimony was plainly partisan. Mr B's evidence was, in the main, honest and frank. However, his reasons for accessing the Respondent's computer and how these related to the search of the email inbox are obscure. TS gave her evidence in a straightforward manner although some detail was lacking, for example, when she was unable to provide examples of documents or cases she had accessed on the Respondent's computer. Overall, the Complainers' witnesses' evidence was in broad agreement with some divergences on minor matters, such as the identities of those authorised to carry out internet banking. In the main, the Tribunal preferred the evidence of the Complainers' witnesses to that of the Respondent and made the findings in fact referred to above. In summary, the Tribunal found that on 28 May 2013, Mr B accessed the Respondent's work computer and found a number of emails from 8 April 2011 to 22 June 2012, some of which referred to TS. These were shown to TS and she was distressed by their content. On 28 May 2013, there was no information security policy in force at the firm and no physical or policy barrier preventing access to the Respondent's computer and his emails.

Parties referred the Tribunal to a number of authorities to assist them in their deliberations. No case was completely on all fours with the present circumstances. Each party sought to distinguish the other's

authorities. However, some general principles could be extracted from disciplinary case law as well as the approach taken in civil and criminal proceedings.

There is no privilege against self-incrimination in disciplinary proceedings (Holder v Law Society 2005 EWHC 2023; MacPherson v Law Society 2005 EWHC and R v ICA ex parte Nawaz 1997 4 WLUK 394). The use of personal emails in disciplinary proceedings is not novel (Craven v Bar Standards Board RCJ 30 January 2014; SRA v West SDT 11470-2016; SRA v Brough, Chaudhary and Story SDT 11380/2015).

In civil proceedings the older practice of the courts was to admit almost evidence which would throw light on disputed facts and enable justice to be done. Evidence illegally or irregularly obtained has been admitted in a number of cases (MacPhail's "Sheriff Court Practice" (3<sup>rd</sup> Edition, 2006) paragraphs 15.109-15.110 and Ratray v Ratray 1897 25R 315). The modern practice is to have regard to the nature of the evidence, the purpose for which it is to be used in evidence, the manner in which it was obtained, fairness to the party from whom it had been illegally obtained, and fairness considered in the light of the matters to be determined in the proceedings as a whole (Walkers "The Law of Evidence in Scotland" (4<sup>th</sup> Edition, 2015) paragraphs 1.7.8; Martin v McGuinness 2003 SLT 1424; Baronetcy of Pringle of Stichill 2016 UKPC 16)

Tribunal proceedings are civil proceedings although they are sometimes called quasi-criminal (Pine v Law Society [2001] EWCA Civ 1574). However, even in criminal cases, an irregularity in obtaining evidence does not necessarily mean that the evidence is inadmissible (Henderson & Marnoch v HMA 2005 HCJAC 47). Considerations to take into account are fairness to the accused, the nature of the irregularity, the circumstances in which it was committed, the whole context in which the evidence came to be created and recovered, the content of the material, the seriousness of the offence, the role of the investigative authorities and the presence or lack of good faith. Evidence which is discovered in an activity which is not itself a search for evidence of criminality is not irregularly obtained, especially where it is discovered by a member of the public (Melville v PF Dundee [2018] SAC (Crim) 14).

Article 8 of the European Convention on Human Rights provides that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. "Private life" is a broad term. Sending and

receiving email is “correspondence” and communications from business premises can relate to “private life”. The fact an email touches on professional and private matters or is sent from a workplace email does not automatically mean it falls outside the scope of “private life”. (Barbulescu v Romania App No 61496/08 and Garamunkanwa v UK ECHR 70571/17). In order to ascertain whether notions of private life and correspondence are applicable, it is relevant to consider whether the individual had a reasonable expectation that his/her privacy would be respected and protected. A reasonable expectation of privacy is a significant but not conclusive factor. It can be relevant that an applicant has not objected to the use or reliance on the material in question when faced with disciplinary proceedings. When assessing whether an individual had a reasonable expectation of privacy, the whole circumstances of the case must be taken into account including the attributes of the claimant, the nature of the activity, the place where it was happening and the nature and purpose of the intrusion. Even if Article 8 is engaged, any interference can be justified by the need to protect the health and welfare of others. (Garamunkanwa v UK ECHR 70571/17).

The Tribunal considered three recent disciplinary cases where other Tribunals had been asked to consider Article 8 arguments regarding the admissibility of emails which were said to have been private.

In Craven v Bar Standards Board RCJ 30 January 2014 the Tribunal rejected the Article 8 argument for exclusion of emails. The emails had been sent from a private address, were unsolicited and were sent to three colleagues (whom the Tribunal treated as members of the public). The email related to business and was not stated to be confidential. The author had no control over what the recipients might do with the material. There was no reasonable expectation of privacy. In any event, use of the emails was in accordance with the law, necessary in a democratic society for the protection of those who wished to use members of the Bar and wished them to have high standards of behaviour as well as being proportionate.

SRA v Brough, Chaudhary and Story SDT 11380/2015, concerned a non-solicitor employee of a firm who accessed internal emails of the Respondents which included insulting and humiliating personal comments about her. The Tribunal recognised that it must have regard to the Respondents’ rights to a fair trial and respect for Article 8 rights. The Tribunal was satisfied that the Respondents intended the emails to be private and did not expect them to be seen by others. However, the exchanges took place on the firm’s email system and were capable of being accessed by individuals in the firm in certain circumstances. The Tribunal did not accept that there was no risk the emails would be read by anyone other than the recipients.

In SRA v West SDT 11470-2016 inappropriate and offensive email correspondence disrespectful of women was carried on with a client using a work email address. The Respondent could reasonably have been expected to anticipate that personal assistants and other colleagues might access the material. He was aware that the firm could access his emails without consent.

The Tribunal also considered the approach of the courts when Article 8 issues are raised regarding admissibility. The facts of these cases were not directly analogous to the present case but demonstrated the approach taken in Article 8 cases.

In Jones v University of Warwick [2003] EWCA Civ 151, hidden film footage was admitted. Fairness was noted to be essential. The court must try to give effect to two competing public interests. The weight to be attached to each will vary according to the circumstances. The significance of the evidence will differ as will the gravity of the breach of Article 8, according to the facts of the particular case. It was noted that it would be artificial and undesirable for actual evidence, which is relevant and admissible not to be placed before the judge who has the task of trying the case. However, it was observed in Martin v McGuinness 2003 SLT 1424 that Jones might have been decided differently in Scotland. It noted that whether Article 8 is infringed depends on the conduct which is the subject of complaint.

In Simpkin v Berkley Group Holdings Plc 2017 EWHC 1472, a document prepared on and sent by an employee from his work computer to his personal email account for a personal purpose was not confidential or privileged. There was no reasonable expectation of privacy. The emails were stored on a central server. His assistant had access to his emails. He had signed an IT policy acknowledging that emails were the property of his employer. His employment contract said that the employer could monitor emails without consent.

Article 8 arguments regarding admissibility also occur in criminal proceedings. The question in Henderson & Marnoch v HMA 2005 HCJAC 47 was whether a lack of authorisation for surveillance could be excused. In that case the Article 8 argument was said to be unsound. The “act” of the Lord Advocate in attempting to lead evidence obtained in breach of Article 8 was “perfectly proper”. The Court held that there was nothing so fundamental about a breach of Article 8 as to make it inappropriate to consider the effect of that breach in relation to Article 6 and the common law principle of fairness.

When considering the Respondent’s first plea-in-law, the Tribunal applied the principles and guidance contained in these cases to the facts it had found. No evidence was led from the other party to the email correspondence, however, it appeared from the circumstances of the case and the Respondent’s evidence

that the emails had been obtained without the authority, knowledge or consent of either correspondent. The Respondent argued that the emails had therefore been “improperly” obtained and should not be admitted to probation.

The Tribunal considered the principles relating to fairness in civil proceedings as laid out in Baronetcy of Pringle of Stichill 2016 UKPC 16. The nature of the evidence was a series of emails between the Respondent and a friend. These were of a personal nature and contained material which might be relevant to a charge of professional misconduct. They had been sent from a work computer. The Tribunal considered the reasons and extent of the search to be relevant factors but recognised that these were not in themselves determinative. Anyone who had access to the office could have accessed these emails. In fact, they were obtained by the office manager. He was said to have been searching for internet banking information. The Tribunal considered that this may not have been his sole reason for accessing the Respondent’s computer. However, he worked in an environment where staff often used others’ computers and there was no physical or policy barrier preventing access. Mr B had a right and implied authority to access the computer. He was perhaps curious regarding the Respondent’s correspondence and took an interest in it beyond simply looking for internet banking information. However, this was not formal monitoring of emails by an employer as in Barbulescu or an illegal search by state officers. It was more akin to the criminal cases where a member of the public stumbles across relevant information which is passed to the authorities. Admission of the emails would throw light on the disputed facts and would enable the disciplinary proceedings to take place. The probative value outweighed any prejudice to the Respondent in the balance of fairness. Therefore, the Tribunal repelled the Respondent’s first plea-in-law.

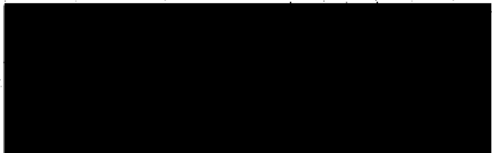
The Tribunal went on to consider the law as it applied to the facts in the light of the Respondent’s second plea-in-law. The Respondent argued that the emails should be excluded on the basis that their use in Tribunal proceedings would infringe the correspondents’ Article 8 rights.

Following the guidance from the European Court of Human Rights in the cases above, and the application of these principles in domestic disciplinary tribunals, the Tribunal considered that the emails in question were capable of falling within the Respondent’s private life and correspondence, despite the fact they had been sent from a work email address and referenced particular cases and the trainee in the Respondent’s workplace. However, the Tribunal did not consider that the Respondent had a reasonable expectation that his privacy would be respected and protected. The Tribunal rejected his evidence that no one should have used his computer. The testimony of the Complainers’ witnesses, which it preferred, was that the use of colleagues’ computers was a frequent occurrence in the office. TS gave evidence

that she had used the Respondent's computer at his request. Mr B gave evidence that the firm used an external IT company which might access the computer. Mr B had previously warned the Respondent regarding other material found on his computer. The Respondent had no control over what happened to the emails after he sent them. The recipient's workplace could have intercepted them, or she could have disseminated them herself. The Respondent's expectation of privacy was not reasonable. The material has been used by several bodies in the course of their investigations and public decisions taken on the basis of the material. The Respondent can no longer have a reasonable expectation that these emails are private.

However, even if Article 8 is engaged, the interference with the Respondent's rights can be justified by the need to protect the health and rights and freedoms of others. TS and the child referred to in the emails are entitled to protection. There is also a public interest in ensuring that solicitors are fit and proper persons to be members of the profession. The use of the emails in these proceedings is in accordance with the law. The Society has a duty to prosecute professional misconduct and to uphold the standards of the profession. The Tribunal's purposes are to protect the public and uphold the reputation of the profession. It is necessary in a democratic society to protect those members of the public using solicitors. It has long been established that a solicitor's private behaviour can constitute professional misconduct. The admission of the emails is necessary and proportionate in the circumstances. Therefore, the Tribunal repelled the Respondent's second plea-in-law.

Parties indicated that two days would be required for a hearing. Dates were canvassed with the parties and the case was continued to a date to be fixed. The Tribunal allowed the Respondent three weeks to lodge full Answers and the Complainers three weeks thereafter to adjust. All questions of expenses were reserved to the conclusion of proceedings. Due to the sensitive nature of the case, all parties except the Respondent and his partner will be anonymised in this procedural decision as publication of their personal data might damage their interests.



**Alan McDonald**  
**Vice Chair**