DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Ms [redacted]

Of: [redacted]

1. The Information Commissioner ("Commissioner") has decided to issue Ms [redacted] ("Ms [redacted]") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the seventh data protection principle by Ms [redacted].

2. This notice explains the Commissioner's decision.

Legal framework

3. Ms [redacted] is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

4. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and

against accidental loss or destruction of, or damage to, personal data".

5. Paragraph 9 at Part II of Schedule 1 to the DPA provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected".

6. Under section 55A (1) of the DPA the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the DPA by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

7. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

8. The DPA implements European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The Commissioner approaches the data protection principles so as to give effect to the Directive.

Background to the case

9. Ms [redacted] is a senior barrister who specialises in family law at [redacted] ("Chambers").

10. On 5 January 2016, a local authority solicitor informed Chambers that documents containing confidential and sensitive information could be accessed on the internet. Further, that the author of the documents

was Ms [redacted]

11. Ms [redacted] had created the documents at home on her standalone desktop computer, mainly for work purposes. They were held in specific files ("files").

12. The desktop computer was password protected but the files were unencrypted.

13. In January 2013, the Bar Council and her Chambers issued guidance to barristers that a computer used by family members or others may in addition require encryption of specific files in order to prevent unauthorised access to confidential material by shared users.

14. Ms [redacted] was aware that her husband had access to the desktop computer via an administration account. He could therefore access Ms [redacted] files without a password, although there is no suggestion that this occurred.

15. Ms [redacted]'s husband wanted to update the software on the desktop computer. On 19 September 2015, he temporarily uploaded Ms [redacted]'s files (725 documents) to an online directory to back them up. He assumed that the documents were safe.

16. However, the documents were visible to an internet search engine and 15 of the documents contained in the folders were cached and indexed. This meant that a document could be easily accessed using a recognisable word, such as a name.

17. Six of the 15 documents contained confidential and highly sensitive information relating to lay clients who were involved in proceedings in

the Court of Protection and the Family Court. Between 200 and 250 individuals were affected by this incident, including vulnerable adults and children.

18. Ms [redacted]'s husband immediately removed the files from the online directory. The internet service provider removed the cached information from the internet the following day.

19. The Commissioner has made the above findings of fact on the balance of probabilities.

20. The Commissioner has considered whether those facts constitute a contravention of the DPA by Ms [redacted] and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

21. The Commissioner finds that Ms [redacted] contravened the following provisions of the DPA:

22. Ms [redacted] failed to take appropriate technical measures against the unauthorised or unlawful processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

23. The Commissioner finds that the contravention is as follows. Ms [redacted] did not have in place appropriate technical measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that her files could not be accessed by unauthorised third parties.

24. In particular, Ms [redacted] did not encrypt the files.

25. This was an ongoing contravention from January 2013 until 5 January 2016 when remedial action was taken.

26. The Commissioner is satisfied that Ms [redacted] was responsible for this contravention.

27. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

28. The Commissioner is satisfied that the contravention identified above was serious due to the number of affected individuals, the nature of the personal data that was contained in the files and the potential consequences. In those circumstances, Ms [redacted]'s failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

29. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contravention of a kind likely to cause substantial distress

30. The relevant features of the kind of contravention are:

31. The files contained confidential and highly sensitive information relating to between 200 and 250 individuals. The files therefore required adequate security measures to protect the personal data.

32. This is all the more so when confidential and highly sensitive information is concerned – in particular, as regards to adults and children in vulnerable circumstances who expected that it would be held securely. This heightens the need for robust measures – in technical terms – to safeguard against unauthorised or unlawful access. Ms [redacted] appears to have overlooked the need to ensure that she had robust measures in place for no good reason.

33. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress to Ms [redacted]'s lay clients if they knew that their confidential and highly sensitive information had been accessed by unauthorised third parties over a three month period.

34. Further, Ms [redacted]'s lay clients would be distressed by justifiable concerns that this information would be further disseminated even if those concerns do not actually materialise.

35. If this information has been misused by the person who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to Ms [redacted]'s lay clients.

36. The Commissioner considers that such distress is likely to be substantial having regard to the number of individuals affected and the nature of the personal data that was contained in the files.

37. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or foreseeable contravention

38. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that Ms [redacted]'s actions which constituted those contraventions were deliberate actions (even if Ms [redacted] did not actually intend thereby to contravene the DPA).

39. The Commissioner considers that in this case Ms [redacted] did not deliberately contravene the DPA in that sense. She considers that the inadequacies outlined above were matters of serious oversight rather than deliberate intent to ignore or bypass the provisions of the DPA.

40. The Commissioner has gone on to consider whether Ms [redacted] knew or ought reasonably to have known that there was a risk that this contravention would occur. She is satisfied that this condition is met, given that Ms [redacted] was aware that her files contained personal data, including confidential and highly sensitive information. Ms [redacted] was also aware that her husband had an administration account that gave him access to the files, and that the Bar Council and her Chambers had issued guidance about this security risk.

41. In the circumstances, Ms [redacted] ought reasonably to have known that there was a risk that such an incident would occur unless she ensured that the files that were held on the desktop computer were technically protected.

42. Second, the Commissioner has considered whether Ms [redacted] knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial distress. She is satisfied that this condition is met, given that Ms [redacted] was aware of the nature of the information that was contained in the files. Ms [redacted] ought to have known that it would cause substantial distress if the information was

used in ways her lay clients did not envisage.

43. Ms [redacted] should also have known that if the data contained in the files has in fact been accessed by untrustworthy third parties then it would cause further distress to Ms [redacted]'s lay clients.

44. Therefore, it should have been obvious to Ms [redacted] that such a contravention would be of a kind likely to cause substantial distress to the affected individuals.

45. Third, the Commissioner has considered whether Ms [redacted] failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances would have entailed encrypting the files. Ms [redacted] did not take that step. The Commissioner considers there to be no good reason for that failure.

46. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.

The Commissioner's decision to issue a monetary penalty

47. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Ms [redacted] with respect to the files. The contravention was of a kind likely to cause substantial distress. Ms [redacted] knew or ought to have envisaged those risks and she did not take reasonable steps to prevent the contravention.

48. The Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. She is also satisfied that section

55A(3A) and the procedural rights under section 55B have been complied with.

49. The latter has included the issuing of a Notice of Intent dated 3 January 2017, in which the Commissioner set out her preliminary thinking.

50. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

51. The Commissioner has considered whether, in the circumstances, she should exercise her discretion so as to issue a monetary penalty. She has taken into account the representations made in response to the Notice of Intent and in other correspondence on this matter.

52. The Commissioner has also considered whether the contravention identified above could be characterised as one-off events or attributable to mere human error. She does not consider that the contravention could be characterised in those ways.

53. The Commissioner has concluded that it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in the circumstances. The contravention is serious in terms of both Ms [redacted]'s deficiencies and the impact such deficiencies were likely to have on the affected individuals.

54. The issuing of a monetary penalty in this case would be fair and just. It would accord with the Commissioner's statutory guidance and regulatory objectives. It would act as an encouragement to ensure that such deficiencies are not repeated elsewhere.

55. For these reasons, the Commissioner has decided to issue a monetary penalty in this case.

The amount of the penalty

56. The Commissioner has taken into account the following **mitigating features** of this case:

- Ms [redacted] has been fully co-operative with the ICO.
- Ms [redacted] has now taken remedial action.

57. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data.

58. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£1,000 (One thousand pounds)**.

Conclusion

59. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **12 April 2017** at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

60. If the Commissioner receives full payment of the monetary penalty by **11 April 2017** the Commissioner will reduce the monetary penalty by

20% to **£800 (Eight hundred pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

61. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

a) the imposition of the monetary penalty and/or;

b) the amount of the penalty specified in the monetary penalty notice.

62. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

63. Information about appeals is set out in Annex 1.

64. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the monetary penalty and any variation of it has expired.

65. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner

as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 10th day of March 2017

Signed [redacted]

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester

LE1 8DJ

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (Information Rights) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).