ico.
Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The Independent Inquiry into Child Sexual Abuse

Of: PO Box 72289, London, SW1P 9LF

1. The Information Commissioner ("the Commissioner") has decided to issue The Independent Inquiry into Child Sexual Abuse ("the Inquiry") 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 the Inquiry.

2. This notice explains the Commissioner's decision.

Legal framework

3. The Inquiry 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. On 7 July 2014, the Inquiry was established to investigate the extent to which institutions have failed to protect children from sexual abuse.

10. [redacted]

11. The Inquiry [redacted] provides a forum for victims and survivors of child sexual abuse. Its participants are provided with regular e-mail updates on the work of the Inquiry.

12. On 27 February 2017, a staff member sent a blind carbon copy ("bcc") e-mail to 90 participants informing them about a forthcoming public hearing. He noticed an error in a link contained within the body of the e-mail and sent a correction by entering the participant's e-mail addresses into the 'to' field instead of the 'bcc' field, by mistake. The recipients of the e-mail could therefore see the e-mail addresses of all the other recipients ("the security breach").

13. 52 of the e-mail addresses contained the full names of the participants or had a full name label attached, and 23 included a partial name.

14. The Inquiry was notified about the security breach by a recipient of the e-mail who entered two further e-mail addresses into the 'to' field before clicking on 'Reply All'. One was a generic contact e-mail address for the Inquiry, and the other was the external e-mail address of an Inquiry panel member.

15. The Inquiry then sent three e-mails to the participants asking them to delete the original e-mail and not to disseminate it further. One of these e-mails generated 39 'Reply All' e-mails from 22 recipients, thereby exacerbating the security breach.

16. Subsequently, the Inquiry instructed the Company that provided its IT services ("the Company") to create and maintain a mailing list for the participants. The Inquiry did not test the functionality of the mailing list before roll-out, and relied on advice provided by the Company that it would prevent individual recipients from replying to the entire mailing list.

17. On 20 July 2017, a recipient clicked on 'Reply All' in response to an e-mail from the Inquiry via the mailing list. This revealed the recipient's e-mail address to the entire mailing list, contrary to the Company's advice. Four more participants revealed their e-mail addresses to the entire mailing list by clicking on 'Reply All' when replying to the recipient's e-mail.

18. The forum registration form also stated that "*any information you provide in this form will be stored securely and not shared with any third parties*". Furthermore, the Inquiry's Privacy Notice stated that the "*Inquiry will keep your information confidential at all* times" and that they would "*treat all the information we receive in the strictest confidence*".

19. Despite this commitment to the participants, the Inquiry disclosed their e-mail addresses to the Company when it outsourced the mailing list, without their consent.

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

21. The Commissioner has considered whether those facts constitute a contravention of the DPA by the Inquiry and, if so, whether the

conditions of section 55A DPA are satisfied.

The contravention

22. The Commissioner finds that the Inquiry contravened the following provisions of the DPA:

23. The Inquiry failed to take appropriate technical and organisational measures against unauthorised processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

    In particular:

    - The Inquiry failed to use an e-mail account that could send a separate e-mail to each participant.
    - The Inquiry failed to provide staff with any (or any adequate) guidance or training on the importance of double checking that the participant's e-mail addresses were entered into the 'bcc' field.

24. This was an ongoing contravention until the Inquiry took effective remedial action following the security breach.

25. The Commissioner is satisfied that the Inquiry was responsible for this contravention.

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

Seriousness of the contravention

27. The Commissioner is satisfied that the contravention identified above was serious. 52 of the 90 e-mail addresses contained the full names of the participants. The recipients of the e-mails could infer that many of the other recipients were victims and survivors of child sexual abuse. This is confidential and sensitive personal data.

28. In the circumstances, the Commissioner considers that the contravention was serious having regard to the number of affected individuals, the nature of the confidential and sensitive personal data involved and the potential consequences.

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 Inquiry sent an e-mail to 90 participants. The recipients of the e-mail could see the e-mail addresses of all the other recipients. They could infer that many of the other recipients were victims and survivors of child sexual abuse. E-mail addresses can also be searched via social networks and search engines.

32. The Commissioner considers that the contravention identified above had the following potential consequences:

33. The contravention would cause distress to at least some of the participants who know that their full names have been disclosed to unauthorised individuals who could infer that they were victims and survivors of child sexual abuse. E-mail addresses can also be searched

via social networks and search engines. It would therefore be possible for the unauthorised individuals to identify some of the affected individuals.

34. It is important to take into account that the Inquiry disclosed the participant's e-mail addresses in contravention of the forum registration form and its own Privacy Notice. The participants are likely to be distressed by a failure to process their data in accordance with their reasonable expectations.

35. Further, the participants would be distressed by justifiable concerns that their data has been further disseminated even if those concerns do not actually materialise.

36. In this context it is important to bear in mind that the participants were suffering from the lifelong consequences of child sexual abuse, and therefore extremely vulnerable. They also had a right to lifelong anonymity.

37. For example, one complainant to the ICO reported that he was "*very distressed*" by the security breach and "*I live in fear of him looking for me*". Further, that "*I sleep with a light on and bolt my bedroom door, I am on medication from my GP who has referred me for counselling and assessment*".

38. If this information has been misused by those who had access to it, or if it was in fact disclosed to hostile third parties, then the contravention would cause further distress to the participants.

39. The Commissioner considers that the distress described above was likely to arise as a consequence of the kind of contravention.

40. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of affected individuals and the confidential and sensitive nature of the personal data involved.

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

Deliberate or negligent contravention

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

43. The Commissioner considers that in this case the Inquiry did not deliberately contravene the DPA in that sense.

44. The Commissioner has gone on to consider whether the contravention identified above was negligent. First, she has considered whether the Inquiry 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 the forum was the only mailing list used by the Inquiry, and an important mechanism by which it engaged with victims and survivors of child sexual abuse.

45. At the time of the security breach, there were 90 participants who received regular e-mail updates from members of staff who used the 'bcc' field to protect the identity of the other recipients. Therefore, the

Inquiry should have been aware that there was a risk that its staff could enter the participant's e-mail addresses into the wrong field.

46. It was also reasonably foreseeable that some of the recipients would click on 'Reply All' and add further e-mail addresses when responding to an e-mail, thereby perpetuating the e-mail chain.

47. It is worth noting that the Commissioner's office issued two monetary penalty notices on 11 December 2015 (Bloomsbury Patients Network) and 4 May 2016 (Chelsea & Westminster Hospital NHS Trust) which raised awareness about the risks of sending bulk e-mails using the 'bcc' field.

48. In the circumstances, the Inquiry ought reasonably to have known that the participant's e-mail addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.

49. Second, the Commissioner has considered whether the Inquiry 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 the Inquiry should have been aware that 52 of the 90 group e-mail addresses contained the full names of the participants. The recipients of the e-mails could infer that many of the other recipients were victims and survivors of child sexual abuse. This is confidential and sensitive personal data. Therefore, it should have been obvious to the Inquiry (in the context of its terms of reference) that such a contravention would be of a kind likely to cause substantial distress to the affected individuals.

50. Third, the Commissioner has considered whether the Inquiry 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 included carrying out a Privacy Impact Assessment at the outset, deciding to use an e-mail account that could send a separate e-mail to each participant, or at the very least providing staff with adequate guidance and training on the importance of double checking that the participant's e-mail addresses were entered into the 'bcc' field. The Inquiry failed to take any of these steps.

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

The Commissioner's decision to impose a monetary penalty

52. The Commissioner has concluded that the conditions for issuing a monetary penalty are in place. She has considered whether it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in this case. Her conclusion is that it is appropriate to do so in all the circumstances. The contravention is serious in terms of both the Inquiry's deficiencies and the impact such deficiencies were likely to (and in this case did) have on the data subjects.

53. 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.

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

- The Inquiry apologised to the affected individuals.
- The Inquiry has now taken substantial remedial action.

- A monetary penalty may have a significant impact on the Inquiry's reputation.
- This security breach has been widely publicised in the media.

55. The Commissioner has also taken into account the following **aggravating features** of this case:

- The Inquiry initially failed to take effective remedial action thereby exacerbating the security breach.
- The Inquiry and the ICO received 22 complaints about the security breach.

56. The Inquiry also contravened the first data protection principle at Part I of Schedule 1 to the DPA by unfairly disclosing the participant's e-mail addresses to the Company when it outsourced the mailing list, without their consent.

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 remind data controllers to ensure that appropriate and effective security measures are applied to personal data.

Conclusion and amount of penalty

58. The Commissioner confirms that she has taken account of the Inquiry's oral and written submissions in response to her Notice of Intent.

59. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.

60. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£200,000 (Two hundred thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

61. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **7 August 2018** 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.

62. If the Commissioner receives full payment of the monetary penalty by **6 August 2018** the Commissioner will reduce the monetary penalty by 20% to **£160,000 (One hundred and sixty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

63. 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.

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

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

66. 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.

67. 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 5th day of July 2018

Signed [redacted].....

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

ico.
Information Commissioner's Office

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)).