Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: [redacted] Historical Society

Of: [redacted]

1. The Information Commissioner ("Commissioner") has decided to issue [redacted] Historical Society ("Historical Society") 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 Historical Society.

2. This notice explains the Commissioner's decision.

Legal framework

3. The Historical Society (an unincorporated association) 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 [redacted] an administrative officer ("Officer") working for the Historical Society left a laptop in [redacted] was broken into and the laptop (among other things) was stolen. The break in was reported to the police but the

laptop has still not been recovered. It was unencrypted.

10. The Historical Society purchased the laptop in [redacted] to enable the Officer to transfer details of the artefacts in its collection from a paper ledger to a digital format.

11. The artefacts were kept in four different locations in [redacted] The Officer took the laptop home before [redacted] weekly visit to one of the locations.

12. The laptop contained (among other things) a list of [redacted] individuals who had donated or loaned artefacts to the Historical Society, including the [redacted]

13. The Officer was using this information to check that artefacts were not double counted.

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

15. The Commissioner has considered whether those facts constitute a contravention of the DPA by the Historical Society and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

16. The Commissioner finds that the Historical Society contravened the following provisions of the DPA:

17. The Historical Society failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

18. In particular:

(a) The Historical Society issued the Officer with an unencrypted laptop.

(b) The Historical Society did not have in place any policies governing the use of encryption, homeworking and the storage of mobile devices.

19. This was an ongoing contravention from [redacted] until remedial action was taken following the security breach.

20. The Commissioner is satisfied that the Historical Society was responsible for this contravention.

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

Seriousness of the contravention

22. The Commissioner is satisfied that the contravention identified above was serious due to the number of affected individuals, the highly sensitive nature of some of the personal data that was held on the laptop and the potential consequences. In those circumstances, the Historical Society's failure to take adequate steps to safeguard against

unauthorised or unlawful access and accidental loss was serious.

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

Contravention of a kind likely to cause substantial damage or substantial distress

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

25. The Officer was required to hold personal data relating to [redacted] individuals on the laptop. Mobile devices such as laptops have a high risk of loss or theft and therefore require adequate security measures to protect the personal data.

26. This is all the more so when information of a highly sensitive nature is concerned – in particular, as regards [redacted] who expected that it would be held securely. This heightens the need for robust measures – in technical or organisational terms – to safeguard against unauthorised or unlawful access and accidental loss.

27. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress to [redacted] if they knew that their [redacted] might have been accessed by an unauthorised third party.

28. Further, [redacted] would be distressed by justifiable concerns that this information would be further

disseminated even if those concerns do not actually materialise.

29. In this context, it is important to bear in mind that [redacted]

30. 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 [redacted] and damage, such as exposing them to [redacted]

31. The Commissioner considers that such damage or distress is likely to be substantial having regard to the number of affected individuals and the highly sensitive nature of some of the personal data that was held on the stolen laptop.

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

Deliberate or foreseeable contravention

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

34. The Commissioner considers that in this case the Historical Society 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.

35. The Commissioner has gone on to consider whether the Historical Society 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 Historical Society was aware that the Officer used an unencrypted laptop to hold personal data, some of which was of a highly sensitive nature relating to [redacted] The Historical Society ought reasonably to have been aware that it needed to ensure so far as possible that the personal data that was held on the laptop was adequately protected.

36. In view of the number of high-profile data losses, the Commissioner's office provided published guidance on its website in 2010 which clearly states that: "In recent years there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access. In many of these cases, these were caused by data being inadequately protected or the devices the data was stored on being left in inappropriate places – and in some cases both. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued".

37. It is worth noting that the Commissioner's office issued two monetary penalty notices on 13 December 2012 (Greater Manchester Police) and 4 June 2013 (Glasgow City Council) which raised awareness about the issue of stolen mobile devices holding personal data.

38. In the circumstances, the Historical Society ought reasonably to have known that there was a risk that this contravention would occur unless

it ensured that the personal data held on the laptop was technically and/or physically protected.

39. Second, the Commissioner has considered whether the Historical Society knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial damage or substantial distress. She is satisfied that this condition is met, given that the Historical Society was aware of the highly sensitive nature of some of the information that was held on the laptop. The Historical Society ought to have known that it would cause substantial distress if the information was used in ways [redacted] did not envisage.

40. The Historical Society should also have known that if the data has in fact been accessed by untrustworthy third parties then it would cause further distress and also damage to [redacted]

41. Therefore, it should have been obvious to the Historical Society that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

42. Third, the Commissioner has considered whether the Historical Society 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 issuing the Officer with an encrypted laptop and putting in place policies governing the use of encryption, homeworking and the storage of mobile devices. The Historical Society did not take those steps. The Commissioner considers there to be no good reason for that failure.

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

The Commissioner's decision to issue a monetary penalty

44. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of the Historical Society with respect to the unencrypted laptop that was issued to the Officer. The contravention was of a kind likely to cause substantial damage or substantial distress. The Historical Society knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. 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.

45. The latter has included the issuing of a Notice of Intent dated 16 May 2016, in which the Commissioner set out her preliminary thinking.

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

47. 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.

48. 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.

49. 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 the Historical Society's deficiencies and the impact such deficiencies were likely to have on the data subjects.

50. 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.

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

The amount of the penalty

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

- The Officer left the laptop in [redacted]
- The laptop was password protected.
- The information has not been further disseminated as far as the Commissioner is aware.
- A monetary penalty may have a significant impact on the Historical Society's reputation.

53. The Commissioner has considered the likely impact of a monetary penalty on the Historical Society. She has decided that the Historical Society has access to sufficient financial resources to pay the monetary penalty without causing undue financial hardship.

54. 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.

55. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£500 (Five hundred pounds)**.

Conclusion

56. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **8 December 2016** 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.

57. If the Commissioner receives full payment of the monetary penalty by **7 December 2016** the Commissioner will reduce the monetary penalty by 20% to **£400 (Four hundred pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

58. 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.

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

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

61. 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.

62. 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 7th day of November 2016

Signed [redacted]

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

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) General Regulatory Chamber (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;

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

e) 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 (General Regulatory Chamber) 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)).