ico.
Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The University of Greenwich

Of: Old Royal Naval College, Park Row, Greenwich, London SE10 9LS

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

2. This notice explains the Commissioner's decision.

Legal framework

3. The University 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. Historically, the University was made up of a number of schools including the Computing and Mathematics School ("the CMS"). The CMS operated an autonomous computer system which was connected to the University's central student management system.

10. In 2012, the University reorganised its structure into four Faculties. The CMS became part of the Architecture, Computing and Humanities Faculty.

11. The CMS had a policy that allowed academics to create microsites (or web pages) on its computer system for specific purposes.

12. In 2004 a student, on behalf of an academic within CMS, developed a bespoke microsite on CMS's web server ("the web server") for the sole purpose of facilitating a training conference.

13. The microsite included a form that permitted anonymous uploads by public URL so that delegates could upload conference papers. Following the conference, the upload function wasn't updated or removed by the student or the academic.

14. In 2013, there is evidence that the microsite was compromised.

15. Between 11 and 16 January 2016, multiple attackers exploited the vulnerability by using SQL injection against the microsite to gain access to an account with sufficient permissions to upload known PHP exploits to the microsite.

16. The PHP exploits permitted access to other areas on the web server, and the attackers were then able to access the databases hosted on the web server ("the web server databases"), [redacted]

17. The Commissioner understands that an attacker accessed and extracted the personal data held on [redacted]

[redacted] relating to approximately 19,500 data subjects including students, alumni, staff, external examiners, applicants and attendees at events ("the security breach").

18. The personal data consisted mainly of contact details such as names, addresses, telephone numbers and email addresses.

19. However, sensitive information was also compromised relating to approximately 3,500 of the data subjects such as extenuating circumstances (e.g. difficult domestic situations and physical or mental health problems), assessment offences, learning difficulties (e.g. dyslexia), food allergies and staff sickness records.

20. On 16 January 2016, an attacker posted the personal data online via Pastebin.com which is used by hackers to publicise their attacks.

21. There is evidence that the microsite was further compromised in April and May 2016.

22. The University first became aware of the security breach on 8 June 2016, following an intense attack on the microsite on 7 June 2016 that resulted in comments on social media, when remedial action was taken.

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

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

The contravention

25. The Commissioner finds that the University contravened the following provisions of the DPA:

26. The University failed to take appropriate technical and organisational 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.

27. The Commissioner finds that the contravention was as follows. The University did not have in place appropriate technical and organisational measures for ensuring so far as possible that such a security breach would not occur, i.e. for ensuring that the web server and [redacted] could not be accessed by attackers using SQL injection.

28. In particular:

    (a) The University was not aware that its infrastructure included a microsite that was vulnerable to SQL injection attack, with access to underlying databases.

    (b) The University did not identify the possible risks to its wider network and underlying systems.

    (c) The University did not ensure that the microsite was decommissioned when it was no longer necessary, or that the microsite was otherwise made secure.

(d) The University did not undertake appropriate proactive monitoring activities to discover vulnerabilities.

29. This was an ongoing contravention from 6 April 2010 when section 55A of the DPA came into force, until the University took remedial action on 8 June 2016.

30. The Commissioner is satisfied that the University was responsible for this contravention.

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

Seriousness of the contravention

32. The Commissioner is satisfied that the contravention identified above was serious due to the number of data subjects, the nature of the personal data that was held on [redacted], and the potential consequences. In those circumstances, the University's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

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

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

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

35. An attacker accessed and extracted the (sensitive) personal data that was held on [redacted] relating to approximately 19,500 data subjects including contact details, and sensitive information relating to approximately 3,500 of the data subjects. [redacted]

36. The information that was obtained was clearly of interest to the attacker given the targeted nature of the attack and that the (sensitive) personal data was subsequently posted online via Pastebin.com. The web server and [redacted] therefore required adequate security measures to protect the personal data.

37. This is all the more so when sensitive information is concerned – in particular, as regards students and members of staff in the University community who expected that it would be held securely. This heightens the need for robust technical and organisational measures to safeguard against unauthorised or unlawful access. For no good reason, the University appears to have overlooked the need to ensure that it had robust measures in place despite having a central IT team.

38. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress. The Commissioner also considers that such distress was likely to be substantial having regard to the number of data subjects and the nature of the personal data that was held on [redacted]

39. If this information has been misused by the persons 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 data subjects and damage such as exposing them to spamming or blagging and possible fraud.

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

Deliberate or negligent contravention

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

42. The Commissioner considers that in this case the University 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.

43. The Commissioner has gone on to consider whether the University 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 University should have been aware that its infrastructure included a microsite that was vulnerable to SQL injection attack, with access to an underlying [redacted] that held (sensitive) personal data, and [redacted]

44. The University should also have known that it was possible for attackers to have further accessed (sensitive) personal data held within [redacted]

45. SQL injection is a common and well-understood security vulnerability, and known defences exist.

46. In 2013, there was evidence that the microsite was compromised.

47. In May 2014, the Commissioner's office issued guidance called 'protecting personal data in online services: learning from the mistakes of others'.

48. The 'SQL injection' section of the guidance – good practice summary states:

"Consider procuring independent security testing (penetration testing, vulnerability assessment, or code review, as appropriate) of the relevant sites or applications in order to identify code development issues, including SQL injection flaws. Do this before the application goes live. It is good practice to periodically test live applications."

49. The 'decommissioning of software or services' section of the guidance, paragraphs 52 to 54 and the first example states:

"Even worse, with the assumption that the legacy site has now been decommissioned, it is now even less likely that the company will arrange for appropriate technical measures to be in place, such as security testing or software update procedures for the legacy site. This means that the likelihood of a compromise will increase over time and any such compromise may not be discovered until a significant time after the attack."

50. In the circumstances, the University ought reasonably to have known that there was a risk that an attack performed by SQL injection would occur unless it ensured that the (sensitive) personal data that was held on [redacted] and [redacted] were technically and organisationally protected.

51. Second, the Commissioner has considered whether the University knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial damage or substantial distress.

52. She is satisfied that this condition is met, given that the University ought to have known that it would cause substantial damage or substantial distress to the data subjects if their (sensitive) personal data was accessed by cyber attackers.

53. Therefore, it should have been obvious to the University that such a contravention would be of a kind likely to cause substantial damage and substantial distress to the data subjects.

54. Third, the Commissioner has considered whether the University 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 being aware of the microsite either in 2004 or in the intervening period; identifying the possible risks to its wider network and underlying systems; ensuring that the microsite was decommissioned when it was no longer necessary, or that the microsite was otherwise made secure; and ensuring that appropriate testing and monitoring was in place. The University did not take those steps. The Commissioner considers there to be no good reason for that failure.

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

56. 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 University with respect to the (sensitive) personal data that was held [redacted]. The contravention was of a kind likely to cause substantial damage and substantial distress. The University knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. The conditions for issuing a monetary penalty are met in this case.

The Commissioner's decision to impose a monetary penalty

57. 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 University's deficiencies and the impact such deficiencies were likely to (and in this case did) have on the data subjects.

58. 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.

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

- The microsite was subjected to multiple criminal attacks.

- The computing departments' academics were experts in software engineering, including how to secure information systems.
- The University notified the Commissioner's office and the data subjects.
- A significant amount of the compromised (sensitive) personal data was historic.
- There is no evidence that the compromised (sensitive) personal data was in fact used for successful fraud activities.
- There is no evidence that the attackers accessed [redacted].
- The University was co-operative during the Commissioner's investigation.
- The University has now taken substantial remedial action.
- A monetary penalty may have a significant impact on the University's reputation and, to an extent, its resources.
- The security breach has been widely publicised in the media.

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

- The University received approximately 200 enquiries from the data subjects, including concerns about the possibility of being spammed.

61. 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

62. The Commissioner confirms that she has taken account of the University's submissions in response to her Notice of Intent.

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

64. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£120,000 (One hundred and twenty thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

65. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **16 June 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.

66. If the Commissioner receives full payment of the monetary penalty by **15 June 2018** the Commissioner will reduce the monetary penalty by 20% to **£96,000 (Ninety six thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

67. 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.

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

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

70. 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.

71. 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 16th day of May 2018

Signed [redacted]...

Stephen Eckersley
Head of Enforcement

ico.
Information Commissioner's Office

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)).