Freedom of Information Act 2000 (Section 50)

Decision Notice

Date 30 March 2009

Public Authority: University of Bradford
Address: Richmond Road
Bradford
West Yorkshire
BD7 1DP

Summary

The complainant made a request under the Freedom of Information Act 2000 (the "Act") to the University of Bradford (the "University") for information held by the University in relation to the use of campus computers to access extremist material in the context of that accessed by four named students together with reports on extremist activity amongst students over the two years prior to the date of the request. The University refused to disclose some of the information it held relevant to the scope of the request as it stated that it was exempt from disclosure under section 40 of the Act. The Commissioner considers that the University correctly applied the section 40(2) exemption by virtue of section 40(3)(a)(i) in this case. The Commissioner considers that the University complied with section 1(1)(a) and (b) of the Act as it confirmed what information it held and provided the information that was not exempt to the complainant prior to internal review. However as the University did not confirm what information it held which was exempt from disclosure within 20 working days of the request the Commissioner considers that the University breached section 10(1) of the Act. The Commissioner also considers that the University breached section 17(1)(b) and (c) as it did not accurately state which exemption applied nor did it explain why the exemption applied in this case within the statutory time for compliance.

The Commissioner's Role

1. The Commissioner's duty is to decide whether a request for information made to a public authority has been dealt with in accordance with the requirements of Part 1 of the Freedom of Information Act 2000 (the "Act"). This Notice sets out his decision.

The Request

2. In an email dated 28 February 2008 the complainant made a request to the University for the following information:

   "I would be grateful if you would provide the information the University holds in relation to the use of campus computers to access extremist material in the context of that accessed by the four students - [named student], [named student], [named student] and [named student] …

   This should include copies [of] any reports the University has produced in relation to the use the four students made of computers and any reports the University has produced on extremist activity among students in the last two years."

3. On 20 March 2008 the University responded to the complainant's request for information. It explained that the University provided electronic communication facilities for its students and staff for university academic or administrative purpose. It clarified that it is not provided for personal use. It explained that whilst an insignificant amount of personal use would be tolerated by the University, users must comply with University Regulations and the law and must not conflict with the business needs of the University in any way. In particular, it must not compromise the University's right of access to material on its facilities or right to monitor internet access through them. It stated that the University reserved the right to monitor, view or use, as it deemed appropriate, any data stored or transmitted using University facilities. It directed the complainant to the University Code of Practice on Information, Access and Security section 3.12 and provided the complainant with a link to this document.

4. The complainant wrote to the University and asked for further clarification in relation to its response. On 3 April 2008 the University continued its response to the complainant. It explained that to release information pertaining to individuals would be a breach of the Data Protection Act (1998) (DPA). It clarified that it had provided information on the University's policy on monitoring the use of websites. It stated that the University was not prepared to release further information on particular cases.

5. On 3 April 2008 the complainant wrote to the University and asked it to provide him with a refusal notice stating which exemptions it was relying upon and why.

6. On 8 April 2008 the University responded to the complainant. The University stated that it could not provide information or policy documents that it did not possess. In particular it clarified that the

University did not have a statement of its practice on monitoring students' website activity. It also stated that to provide the information it did hold would infringe section 40 of the Act. It explained that in terms of general policy on extremism on campus, the University follows the guidance issued by Universities UK.

7. The University explained that it provided the police with reports covering log in and log out times of the computer accounts of the students who were the subject matter of the complainant's request. This disclosure was in connection with a police investigation. It clarified that the University did not provide information on the websites visited as that information was not logged. It stated that the University did not possess a copy of the statement made by the University's Head of Technical Services which was read out during a later court case.

8. On 9 April 2008 the complainant asked the University to conduct an internal review.

9. On 10 April 2008, the University wrote to the complainant with the result of the internal review it had carried out. It concluded that the grounds for a partial refusal were correct. It clarified that documentation of the type requested did not exist. It explained that there was information provided to the police relating to the four named students. However the University concluded that to provide this information would contravene section 40(3)(a)(ii) of the Act. In connection with its decision it explained that universities had procedures relating to freedom of speech within the law. Furthermore it went on to explain that staff and students would from time to time have legitimate grounds for access to highly sensitive materials and gave an example of individuals studying Peace Studies. Finally it explained that its staff and students use computing equipment for the purposes of teaching, learning, research and administration. It is accepted that there will be a certain amount of private use which, provided it is of modest level, will be accepted.

The Investigation

Scope of the case

10. On 16 April 2008 the complainant contacted the Commissioner to complain about the way his request for information had been handled. The complainant specifically asked the Commissioner to investigate what information was held by the University under section 1(1)(a) of the Act and furthermore in respect of the information it had confirmed it held but was not willing to disclose, whether it had correctly applied the section 40(2) exemption.

11. The Commissioner also considered whether the University had responded to the complainant's request in compliance with section 10(1) and 17(1)(a), (b) and (c) of the Act.

Finding of Fact

12. The four named students relevant to this complaint were the subject of a police investigation into charges of terrorism. The four named students were convicted at a later criminal trial. However the four named students were cleared on appeal in February 2008.

Chronology

13. On 28 April 2008 the Commissioner wrote to the University to inform it that he had received a complaint from the complainant and that the case was eligible for investigation.

14. On 8 May 2008 the University wrote to the Commissioner. The University explained that the complainant's request dated 28 February 2008 focused on the use of campus computers to access extremist material in the context of that accessed by four students who were recently acquitted on appeal regarding terrorism charges. The University explained that it responded to that request by providing a weblink to the University's Code of Practice on Information Access and Security. It was explained that the University was not in a position to provide information which was no longer in its possession because it had been handed over to the Courts. In addition it clarified that the computer hard drives in question were confiscated by the police and the University's Senior Technical Officer confirmed that the computer accounts in question were not monitored for misuse but the log in and out times had been given to the police as part of their investigations.

15. It explained that it could confirm that there had been many discussions around extremism. However it had not produced any reports or documentation pertaining to extremism involving students on campus.

16. The University referred to another wider request on this issue which had been made by the complainant to the University on 30 April 2008. This was a request for any information held on extremist activity in the last two years. This later wider request has been dealt with as a separate case under the reference FS50201558 and therefore is not considered any further in this notice.

17. However in relation to the part of the complainant's request of 28 February 2008 for any reports produced by the University on extremist activity among any students in the last two years the University did provide the following explanation. It stated that the

Pakistan Security Research Unit in its Department of Peace Studies worked closely with other agencies and has as part of its research produced reports on the subject of extremism and terrorism in Pakistan. The University provided a link to these reports but explained that they did not relate to extremist activities on campus within two years of the date of the request.

18. On 15 November 2008 the Commissioner wrote to the University. The Commissioner wished to determine what information the University held relevant to the scope of the complainant's request under section 1(1)(a) of the Act. In relation to this part of the investigation the Commissioner asked the University for clarification in relation to the following points:-

- What information was held relevant to the scope of the complainant's request?
- Whether there was any other information ever held other than that which it declares in response to the bullet point above?
- If so when had it ceased to retain this information?
- Did it have a record of any such documents destruction?
- What did its formal records management policy say about the retention and deletion of records of this type?
- What steps had been taken to locate the requested information? It was asked to provide a detailed account of the searches that had been conducted.
- Finally the Commissioner asked whether there were any statutory requirements to keep the information requested?

19. In relation to information which the University had stated was held but which had been withheld, the Commissioner explained that he had been asked to consider whether or not the University was correct to apply the exemption contained at section 40(2) (by virtue of section 40(3)(a)(i) or (ii)). The Commissioner asked the University for clarification in relation to the following points:-

- What information was it withholding under section 40 of the Act?
- The University was asked to provide copies of all of the "withheld" information.
- It was noted that in its internal review that the University had relied upon the exemption contained at section 40(2) by virtue of section 40(3)(a)(ii). Section 40(3)(a)(ii) relates to section 10 of the Data Protection Act 1998 (DPA). Section 10 of the DPA relates to a data subjects right to provide a notice in

writing to a data controller requiring the data controller to cease to process his or her personal information if processing is likely to cause damage or distress. Therefore the University was asked whether such a notice or notices had been served upon it?

- Alternatively the Commissioner suggested that if the University was actually referring to section 40(3)(a)(i) (which relates to the data protection principles), it was asked to explain why disclosing this information would breach any of the data protection principles which are contained in schedule 1 of the DPA?
- The Commissioner asked whether disclosure of the information would breach any of the data protection principles and whether any of the Schedule 2 Conditions could be met?

20. On 29 December 2008 the University responded to the Commissioner. The University confirmed that the information it held relevant to the scope of the request was computer log in and log out dates and times relating to the individual students named in the request. It explained that students were given a personal email account with a personal password when they enrolled at the University. It clarified that the use of email by students and the University is governed by University Regulation 21 and the Code of Practice for Information Access and Security. This had been provided to the complainant and a link was provided to Regulation 21[1]. It explained that six specific transaction reports were released to the police as part of their investigation. The University confirmed that the records of this exist within the University IT system but are not routinely processed and are designed for audit purposes. The University explained that the reports produced for the police together with the actual PCs had been taken away by police. The University explained that it also processed and provided reports of the students computer accounts to the police and those reports were not retained by the University. It clarified that no other information was held. It stated that the information held was passed to the complainant.

21. The University explained that the steps it had taken to locate the information included the Legal and Governance Officer contacting key personnel across the University to inform them of the request and to obtain information. The key personnel were identified in accordance with the subject matter and included members of the University's senior management team, IT colleagues and academic schools.

[1] http://www.brad.ac.uk/lss/regulations/policy/reg21.php

22. The University confirmed that there were no statutory requirements for it to record the information requested.

23. It confirmed that the information it was withholding was the data held by its IT system which related to the personal email accounts of the students and was accessed and processed at the request of the police as part of their investigation. The University clarified that it could process this report again and asked the Commissioner to confirm if he wished it to do so. The Commissioner understands that this information is the log in and log out dates and times of the four named students.

24. The University confirmed that a section 10 DPA notice had not been served upon the University.

25. Finally the University explained that the information not provided to the complainant was information on the IT system, not in a processed form and was personal to the email accounts of the students. It explained that it had previously been processed at the lawful request of the police. The University argued that to perform a further processing exercise would have breached the terms of the University Regulation 21 and the Code of Practice and the Data Protection Principles.

26. On 9 January 2008 the Commissioner responded to the University and asked some further questions. The Commissioner asked the University to clarify exactly what information had already been provided to the complainant. The University was also asked to produce and provide a copy of the 6 specific transaction reports and the reports of the student's computer accounts which were provided to the police. Finally the University was asked to confirm that there was no further information held other than that which had been provided to the complainant or that which was being withheld under section 40(2) by virtue of section 40(3)(a)(i).

27. On 23 January 2008 the University responded to the Commissioner's further questions. It explained that the information provided to the complainant included a hyperlink to the University's Code of Practice for Information Access and Security. Furthermore the University explained that it advised the complainant that in terms of general policy on extremism it followed guidance issued by Universities UK. The University explained to the complainant that log in/log out times of computer accounts of the individual students referred to within the request were provided to the police. However this is the information which was withheld under section 40(2) by virtue of section 40(3)(a)(i). The University confirmed that it had advised the complainant that there was no other information/documentation available.

28. The University explained that the report supplied by IT Services to the police is an extract of an electronic record held on its IT System. The police were provided with a report for six named students log in and log out dates and times (from a date when the students started at University until the date they were arrested). At the request of the Commissioner the University had run the same report on the 14 January 2009 and this was provided to him. The report only showed log in dates and times and log out dates and times together with the computer used. It did not contain details of the websites accessed by the user.

29. On 29 January 2009, during a telephone conversation with the University, the Commissioner noted that the information showed when the particular students had accessed a university computer. It did not show whether they had accessed any extremist material. The Commissioner asked whether the University could retrieve information as to what sites were accessed. The University explained that it did not monitor user's activities as a matter of course but explained that this did not mean that it couldn't do so. The University explained that the computers seized by the police had now been returned and it would liaise with its IT department to determine whether it would be possible to obtain information from the returned computers.

30. On 2 February 2009 the University wrote to the Commissioner and explained that the relevant PC was seized from a shared cluster in the University's JB Priestley Library. It explained that the PC would have been configured with a standard set of applications as it was available for any registered user to use. The University explained that it used disk imaging techniques during installation to ensure that all of the PCs were identical, and software policies and permissions attempted to keep them that way. The PCs still however deteriorate with use and often have remnants, such as temporary files and partial downloads left on them when a user ends their session. The University explained that it re-images the PCs every few weeks to try to ensure that they remain in reasonable working order. This is an automatic process and it does not record the contents of the PC before rebuilding it. The University's position is that work shouldn't be left on the cluster PCs as all users have access to a networked file store, and any loss of data that way is simply unrecoverable. The University stated that it did not know what the police found on the seized PC, if anything. The University speculated that the police could have used forensic techniques to recover information that had been deleted.

31. The University explained that in addition to seizing the PC, the police also asked for access to the students' personal networked file store but it was not aware what the police may have found in these. As described above the University stated that it configured cluster PC applications to use the networked file store instead of the local

hard drive, so it would be quite likely that information such as the web browser history and favourites, or transcripts of instant messaging sessions would have been found there. The University confirmed that the situation had not changed significantly since that incident.

32. The University also looked at the issue as to whether now that the computers had been returned, could it interrogate the computers to find out whether the users relevant to the complainant's request accessed extremist web sites. The University explained that the police had held the PC for many months and it was not returned until after the trial. The PC was then re-imaged ready to be put back into service, effectively destroying any information that was on it.

33. In relation to the students' network file store, the University explained that this is held centrally so it can be searched if necessary. However the University had been advised by its legal team that generally this should not be done without reasonable grounds as the users have an expectation of privacy. In this particular case at the time of the incident the police were already investigating the incident so there seemed to be no grounds for the University to carry out its own independent enquiries. The University explained that its data backup policy is to retain selected copies of the file store for twelve months for disaster recovery purposes.

34. It explained that this is part of its normal data backup procedure. It takes full backup copies of all data on all major servers every weekend (some of the very large servers are done every two weeks with a consolidation in the middle week) and incremental backups every night. Some of the weekly/fortnightly full dump sets are "better" than others due to various operational issues such as errors and faults that cause backups to fail or be delayed. A set of good full backups from around the middle of the month (depending on when the fortnightly systems fall) are copied to a separate set of tapes that are then taken out of circulation. These copies are placed in another campus location for a month, then spend a further eleven months in the tape store before being returned to service and reused. The tapes have unique labels and their overall table of contents remains in the backup system, but the individual file indexes of the tapes are discarded. This means that the older copies are only useful for extreme disaster recovery purposes as it would take a long time to rescan the tapes to recover the index entries before they can be used. As the last user accessed the system in March 2006 it would not have been possible at the time of the request in February 2008 to go back to the state the file system was in at the time of the last log on.

35. The University confirmed that the PC was returned to the University during late September 2007 and collected by IT Services on 1

October 2007. The University did not have an exact date for its re-image because the PC was missing a few internal components when it was returned and had to be repaired. The University stated that the PC was currently in service at its School of Management Library.

36. On 5 February 2009 the Commissioner wrote again to the University. The Commissioner noted that in an email dated 30 April 2008 from the University to Mr Waugh, it was stated that "All other recorded information which relates to the issue of extremism are part of the High Court records, such information includes statements from our Computer Centre [including the Head of Technical Services statement which was read out in court discussed at paragraph 7 of this notice]. The computer hard drives were confiscated as part of the investigation and we only supplied log in and log out times…." The Commissioner explained that he considered that the University had dealt with the issue of the computer hard drives and the log in and log out times document however he had not seen a copy of the statements from the University's computer centre. The Commissioner therefore asked for a copy of these statements.

37. On 13 February 2009 the University responded to the Commissioner. It stated that those statements were not held by the University at the time of the request. It explained that the Police approached members of staff who were asked to make statements for the purposes of the police investigation, however, the University was not given copies of those statements.

Analysis

Procedural matters

Section 1

38. Section 1(1) of the Act states that:

> *"Any person making a request for information to a public authority isentitled –*
>
> *(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and (b) if that is the case, to have that information communicated to him."*

39. The Commissioner has considered whether the University has complied with section 1(1)(a) and (b) of the Act.

40. The University provided a link to its Code of Practice on Information Access and Security to the complainant on 20 March 2008 and on 3 April 2008 stated that it was not willing to release further information on particular cases as it would be a breach of the DPA. It wasn't until the 8 April 2008 when the University attempted to confirm what information it held relevant to the scope of the request, that being the report on the log in and log out times of the named students, and applied a particular exemption, that being section 40.

41. In relation to the part of the complainant's request of 28 February 2008 for any reports produced by the University on extremist activity among any students in the last two years the University provided the following explanation to the Commissioner on 8 May 2008. It stated that the Pakistan Security Research Unit in its Department of Peace Studies worked closely with other agencies and has as part of its research produced reports on the subject of extremism and terrorism in Pakistan. The University provided a link to these reports but explained that they did not relate to extremist activities on campus within two years of the date of the request. Upon this basis the Commissioner does not consider that the University has produced any reports on extremist activity among students in the last two years (prior to the date of the request) at the University. Therefore the Commissioner is satisfied that this information is not held.

42. In relation to whether the University held any information on the websites accessed by any of the four named students the Commissioner has considered the University's response set out at paragraphs 29 to 35 above. The University confirmed that the PC (that was seized by police) was returned to the University during late September 2007 and collected by IT Services on 1 October 2007. The University did not have an exact date for its re-image because the PC was missing a few internal components when it was returned and had to be repaired. The University looked at the issue as to whether when the computers had been returned, could it interrogate the computers to find out whether the users relevant to the complainant's request accessed extremist web sites. The University explained that the police had held the PC for many months and it was not returned until after the trial. The PC was then re-imaged ready to be put back into service, effectively destroying any information that was on it. The University stated that the PC was currently in service at its School of Management Library. Upon this basis the Commissioner is satisfied that although the actual computer (which had been seized by the police) was returned to the University at the time of the request it would not have been possible to retrieve information as to what websites were visited. This is because the University re-imaged the PC around October 2007 in order to put it back into service.

43. In relation to whether or not the University could have accessed the student network file store to determine what websites were visited, the University has explained that it would be possible to do so. However it explained that its data backup policy is to retain selected copies of the file store for twelve months for disaster recovery purposes. The four named students were arrested in March 2006 which is effectively the last time they accessed the University computers. Therefore even if some information had been retained for twelve months relating the four named students network file store, it would not have been held at the time of the request in February 2008. Upon this basis the Commissioner is therefore satisfied that this information is not held.

44. In relation to statements made by the University's computer centre (including the Head of Technical Services statement which was read out in court), the Commissioner is satisfied that these were not held by the University as they were statements taken by the police.

45. The Commissioner is satisfied from the responses the University has provided to him that the log in and log out dates and times of the named students is all of the information held by the University relevant to the scope of the request.

46. The Commissioner considers that the University confirmed what information it held relevant to the scope of the request and provided the information to the complainant that it was not withholding under section 40 of the Act prior to the internal review. Therefore the Commissioner does not find that section 1(1)(a) or (b) has been breached in this case.

Section 10

47. Section 10(1) of the Act requires that a public authority must comply with section 1(1) promptly and in any event not later than the twentieth working day following the date of receipt of the request.

48. As the University did not confirm exactly what information it held nor applied a particular exemption until 8 April 2008, the Commissioner considers that it did not comply with section 1(1)(a) within 20 working days of the date of the request. As the University provided the information it held which was not exempt from disclosure on 20 March 2008 the Commissioner considers that the University did comply with section 1(1)(b) within 20 working days.

49. As the University did not comply with section 1(1)(a) within 20 working days the Commissioner considers it breached section 10(1).

Section 17

50. Section 17(1) states that –

> *"A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision of Part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which -*
>
> *(a) states that fact,*
>
> *(b) specifies the exemption in question, and*
>
> *(c) states (if that would not otherwise be apparent) why the exemption applies."*

51. The Commissioner has considered whether the University has complied with section 17(1)(a), (b) and (c) of the Act.

52. In this case the University stated that it wished to rely upon the section 40 exemption within its response to the complainant of 8 April 2008. At internal review the University upheld its decision to withhold the information however it incorrectly stated that it was doing so by virtue of section 40(3)(a)(ii). This relates to a section 10 notice under the DPA, this is a notice which is served upon a data controller by a data subject asking that data controller not to process the data subjects personal information as it may cause damage or distress. The University later confirmed to the Commissioner that no such notice had been served.

53. Furthermore the Commissioner considers that the University did not provide the complainant with an adequate or relevant explanation as to why the section 40(2) exemption by virtue of section 40(3)(a)(i) was engaged within the statutory time period.

54. The Commissioner therefore considers that the University breached section 17(1)(b) and (c) as it did not comply with its obligations imposed by these sections within the statutory time for compliance.

Exemption

Section 40(2) by virtue of 40(3)(a)(i)

55. Section 40(2) of the Act provides an exemption for information that constitutes the personal data of third parties:

> *"Any information to which a request for information relates is also exempt information if—*
>
> *(a) it constitutes personal data which do not fall within subsection (1),*

and
(b) either the first or the second condition below is satisfied."

56. Section 40(3)(a)(i) of the Act states that:

> *"The first condition is-*
>
> *(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-*
>
> *(i) any of the data protection principles, or*
> *(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress),"*

57. The full text of section 40 can be found in the legal annex attached to this decision notice.

58. In this case ultimately the University argued that the requested information constituted the personal data of the named students and was therefore exempt under section 40(2) of the Act by virtue of section 40(3)(a)(i) as to release the information would breach the data protection principles. In order to reach a view on the University's arguments the Commissioner has first considered whether the withheld information is the personal data of a third party. Section 1 of the DPA defines personal data as information which relates to a living individual who can be identified:

- from that data, or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

In this instance the information withheld is a list of the names of the students along with the dates and times they accessed campus computers at the University. The Commissioner believes that the named students would be identifiable from this information, and therefore he is satisfied that it is the personal data of the named students.

59. Such information is exempt if either of the conditions set out in sections 40(3) and 40(4) of the Act are met. The relevant condition in this case is at section 40(3)(a)(i) of the Act, where disclosure would breach any of the data protection principles. The University has not specified which principles would be breached however the Commissioner has first considered whether disclosure of the personal data would breach the first data protection principle, which states, amongst other things that, "Personal data shall be

processed fairly and lawfully". Furthermore at least one of the conditions in Schedule 2 should be met.

60. In reaching a decision as to whether disclosure of the requested information would contravene the first data protection principle the Commissioner has considered the following:-

How was the information obtained?

61. The information was obtained because the named students who were enrolled to study at the University accessed its computers. This is something that all students of the University are able to do whilst enrolled there.

62. The Commissioner considers that the named students required access to the University computers as part of the courses they were studying.

63. The log in and log out reports were originally obtained by the University for purposes related to operation, monitoring and security of its computer systems. They were subsequently provided to the police for use in a police investigation.

Likely expectation of the data subject

64. The Commissioner is of the view that the named students are private citizens who were studying at the University. The Commissioner does not consider that they would have expected that their names along with the times and dates they accessed University computers would be put into the public domain. The Commissioner considers that this is not something that any student studying at a University would expect.

65. In determining the above the Commissioner has looked at the Guidance which he has issued which differentiates between and individual's public and private life. This Guidance can be accessed at the following link:-

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/personal_information.pdf

Upon consideration of the Guidance the Commissioner believes that disclosure of the log in and log out dates and times of the four students would be unwarranted as it would reveal information about what the students were doing when and it is information solely relevant to their private lives and does not encompass any form of public function or duty.

66. The Commissioner has considered whether despite the limitation of students expectations, there is an overriding reason why it would nevertheless be fair to make details of the log in/log out times available to the public. In this connection the Commissioner notes again that although the named students were the subject of a highly publicised criminal trial they were ultimately cleared of all charges on appeal. As the named students were cleared of all charges the Commissioner considers that this further supports his view that the named students would not expect nor would wish the requested information to enter the public domain.

67. Having considered the information involved and the purposes for which it was generated, the Commissioner has concluded that it would be unfair and therefore a breach of the first data protection principle to disclose it. Accordingly, he has decided that the information should not be disclosed due to the exemption contained section 40(2) by virtue of section 40(3)(a)(i).

68. As the Commissioner considers that it would be unfair to disclose the requested information he has not gone on to consider the Schedule 2 conditions.

The Decision

69. The Commissioner's decision is that the University dealt with the request for information in accordance with section 1(1)(a) and (b)of the Act.

70. As the University failed to comply with the requirements of section 1(1)(a) within the statutory time for compliance it breached section 10(1) of the Act.

71. The Commissioner considers that the University correctly applied the exemption contained at section 40(2) by virtue of section 40(3)(a)(i) to the withheld information.

72. The Commissioner considers that the University breached section 17(1)(b) and (c) as it failed to accurately specify the exemption it was relying upon, nor did it provide any explanation to the complainant as to why it believed the exemption applied within the statutory time for compliance.

73. The Commissioner also considers that by failing to provide particulars of any procedure provided by the authority for dealing with complaints about requests, and particulars of the rights conferred by section 50, the authority breached section 17 (7) (a) and (b).

Steps Required

74. The Commissioner requires no steps to be taken.

Other Matters

75. Although they do not form part of this Decision Notice the Commissioner wishes to highlight the following matters of concern:

76. As the University did not in its initial response treat the complainant's request as a request under the Act, the Commissioner wishes to remind the University that such correspondence should always be treated as an FOI request and that the onus is upon it to realise this.

77. The Commissioner notes that the outcome of the internal review, as communicated to the requester on the 10 April 2008, did not conform to part VI of the section 45 Code of Practice in as far as it failed to thoroughly review the handling issues associated with the initial request, and did not provide details of the rights of appeal conferred by section 50.

The section 45 Code can be viewed at:

http://www.dca.gov.uk/foi/reference/imprep/codepafunc.htm

Right of Appeal

78. Either party has the right to appeal against this Decision Notice to the Information Tribunal. Information about the appeals process may be obtained from:

Information Tribunal
Arnhem House Support Centre
PO Box 6987
Leicester
LE1 6ZX

Tel: 0845 600 0877
Fax: 0116 249 4253
Email: informationtribunal@tribunals.gsi.gov.uk.

Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Decision Notice is served.

Dated the 30th day of March 2009

Signed ……..

David Smith
Deputy Commissioner

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Legal Annex

General Right of Access

Section 1(1) provides that -
"Any person making a request for information to a public authority is entitled –

(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

(b) if that is the case, to have that information communicated to him."

Section 1(2) provides that -
"Subsection (1) has the effect subject to the following provisions of this section and to the provisions of sections 2, 9, 12 and 14."

Section 1(3) provides that –
"Where a public authority –

(a) reasonably requires further information in order to identify and locate the information requested, and

(b) has informed the applicant of that requirement,

the authority is not obliged to comply with subsection (1) unless it is supplied with that further information."

Section 1(4) provides that –
"The information –

(a) in respect of which the applicant is to be informed under subsection (1)(a), or

(b) which is to be communicated under subsection (1)(b),

is the information in question held at the time when the request is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is to be communicated under subsection (1)(b), being an amendment or deletion that would have been made regardless of the receipt of the request."

Section 1(5) provides that –
"A public authority is to be taken to have complied with subsection (1)(a) in relation to any information if it has communicated the information to the applicant in accordance with subsection (1)(b)."

Section 1(6) provides that –
"In this Act, the duty of a public authority to comply with subsection

(1)(a) is referred to as “the duty to confirm or deny”.”

Time for Compliance

Section 10(1) provides that –
“Subject to subsections (2) and (3), a public authority must comply with section 1(1) promptly and in any event not later than the twentieth working day following the date of receipt.”

Section 10(2) provides that –
“Where the authority has given a fees notice to the applicant and the fee paid is in accordance with section 9(2), the working days in the period beginning with the day on which the fees notice is given to the applicant and ending with the day on which the fee is received by the authority are to be disregarded in calculating for the purposes of subsection (1) the twentieth working day following the date of receipt.”

Section 10(3) provides that –
“If, and to the extent that –

(a) section 1(1)(a) would not apply if the condition in section 2(1)(b) were satisfied, or
(b) section 1(1)(b) would not apply if the condition in section 2(2)(b) were satisfied,

the public authority need not comply with section 1(1)(a) or (b) until such time as is reasonable in the circumstances; but this subsection does not affect the time by which any notice under section 17(1) must be given.”

Section 10(4) provides that –
“The Secretary of State may by regulations provide that subsections (1) and (2) are to have effect as if any reference to the twentieth working day following the date of receipt were a reference to such other day, not later than the sixtieth working day following the date of receipt, as may be specified in, or determined in accordance with the regulations.”

Section 10(5) provides that –
“Regulations under subsection (4) may –

(a) prescribe different days in relation to different cases, and
(b) confer a discretion on the Commissioner.”

Section 10(6) provides that –
“In this section –
“the date of receipt” means –

(a) the day on which the public authority receives the request for information, or
(b) if later, the day on which it receives the information referred to in section 1(3);

"working day" means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom."

Refusal of Request

Section 17(1) provides that -
"A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision of Part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which -

(a) states that fact,

(b) specifies the exemption in question, and

(c) states (if that would not otherwise be apparent) why the exemption applies."

Section 17(2) states –

"Where–

(a) in relation to any request for information, a public authority is, as respects any information, relying on a claim-
(i) that any provision of part II which relates to the duty to confirm or deny and is not specified in section 2(3) is relevant t the request, or
(ii) that the information is exempt information only by virtue of a provision not specified in section 2(3), and

(b) at the time when the notice under subsection (1) is given to the applicant, the public authority (or, in a case falling within section 66(3) or (4), the responsible authority) has not yet reached a decision as to the application of subsection (1)(b) or (2)(b) of section 2,

the notice under subsection (1) must indicate that no decision as to the application of that provision has yet been reached and must contain an estimate of the date by which the authority expects that such a decision will have been reached."

Section 17(3) provides that -

"A public authority which, in relation to any request for information, is to any extent relying on a claim that subsection (1)(b) or (2)(b) of section 2 applies must, either in the notice under subsection (1) or in a separate notice given within such time as is reasonable in the circumstances, state the reasons for claiming -

(a) that, in all the circumstances of the case , the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether the authority holds the information, or

(b) that, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information."

Section 17(4) provides that -

"A public authority is not obliged to make a statement under subsection (1)(c) or (3) if, or to the extent that, the statement would involve the disclosure of information which would itself be exempt information.

Section 17(5) provides that –

"A public authority which, in relation to any request for information, is relying on a claim that section 12 or 14 applies must, within the time for complying with section 1(1), give the applicant a notice stating that fact."

Section 17(6) provides that –

"Subsection (5) does not apply where –

(a) the public authority is relying on a claim that section 14 applies,

(b) the authority has given the applicant a notice, in relation to a previous request for information, stating that it is relying on such a claim, and

(c) it would in all the circumstances be unreasonable to expect the authority to serve a further notice under subsection (5) in relation to the current request."

Section 17(7) provides that –

"A notice under section (1), (3) or (5) must –

(a) contain particulars of any procedure provided by the public authority for dealing with complaints about the handling of requests for information or state that the authority does not provide such a procedure, and

(b) contain particulars of the right conferred by section 50."

Personal information.

Section 40(1) provides that –
"Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject."

Section 40(2) provides that –
"Any information to which a request for information relates is also exempt information if-

(a) it constitutes personal data which do not fall within subsection (1), and
(b) either the first or the second condition below is satisfied."

Section 40(3) provides that –
"The first condition is-

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-

(i) any of the data protection principles, or
(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded."

Section 40(4) provides that –
"The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data)."

Section 40(5) provides that –

"The duty to confirm or deny-

(a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1), and
(b) does not arise in relation to other information if or to the extent that either-
  (i) he giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or
  (ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed)."

Section 40(6) provides that –
"In determining for the purposes of this section whether anything done before 24th October 2007 would contravene any of the data protection principles, the exemptions in Part III of Schedule 8 to the Data Protection Act 1998 shall be disregarded."

Section 40(7) provides that –
In this section-

"the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;
"data subject" has the same meaning as in section 1(1) of that Act;
"personal data" has the same meaning as in section 1(1) of that Act.