First-tier Tribunal
(General Regulatory Chamber)
Information Rights

Appeal Reference: EA/2019/0362

Heard at London (Field House)
On 20 February 2020

Before

KAREN BOOTH
JUDGE

ANDREW WHETNALL and DAVE SIVERS
TRIBUNAL MEMBERS

Between

YVONNE AMEYAW

Appellant

and

THE INFORMATION COMMISSIONER

Respondent

DECISION AND REASONS

This Decision has been corrected (paragraph 31 only) by me under rule 40 of the 2009 procedural Rules.
Karen Booth,
Tribunal Judge
23/6/2020

DECISION

(*NB in this Decision: The Respondent is referred to as "the Commissioner"; the Ministry of Justice is referred to as "the MoJ"; the Data protection Act 1998 is referred to as "the DPA"; and the Freedom of Information Act 2000 is referred to as "FOIA").*

1. The decision notice issued by the Commissioner on 2 September 2019 (reference: FS50762699) is in accordance with the law and the appeal is dismissed.

REASONS

Background to the appeal

The Employment Tribunal claims

2. The Appellant was employed by Pricewaterhousecoopers Services Ltd ("PWC") from April 2014. In 2015/16 she initiated proceedings against PWC in the Employment Tribunal. Her claims were made under the Equality Act 2010 for direct discrimination and harassment, based upon the protected characteristics of race and sex, including victimisation.

   On 31/1/17, there was a preliminary hearing in connection with those claims at the Employment Tribunal in Croydon, before Judge Hall-Smith. Feelings were running high at that hearing and the Judge's reasons refer to disruptive conduct on the part of the Appellant and a relative of hers who accompanied her at the hearing. At some point, a court security officer was called. The incident report subsequently completed by that security officer is at the heart of this appeal.

3. On 3/2/17, PWC suspended the Appellant and on 6/2/17 applied to have her claims struck out by reason of her conduct at the preliminary hearing. That application was refused by Employment Judge Morton on 17/3/17[1], who found that the Appellant's conduct was unacceptable at times but not to such a degree that it would make a fair trial impossible:

> *"19. My conclusion from the materials on which I based this decision is that the Claimant undoubtedly lost her cool at times during the hearing and behaved reprehensively but did not do so without justification. Something had broken down in her communication with her solicitors and she found herself at a hearing with matters not proceeding in accordance with her instructions. [X's] intervention plainly was disgraceful and singularly unhelpful and I am reassured by Mr Herbert's assurance that [X] will not be participating in any future proceedings in this case. However, all are agreed that [X's] conduct cannot be attributed to the Claimant. The Claimant's conduct on its own, although at time uncontrolled and unacceptable, does not in my view on these*

[1] https://assets.publishing.service.gov.uk/media/58d52380ed915d06b0000010/Ms_Y_Ameyaw_v_Pricewaterhousecoopers_Services_Ltd_2302806-2015_and_others_Preliminary.pdf

particular facts amount to conduct that is so exceptional that I need not consider whether a fair trial is still possible.

4. The substantive hearing of the Appellant's claims took place over 8 days in April/May 2017. In a reserved judgement dated 7/3/18, the employment tribunal dismissed all her claims[1].

5. Following an internal investigation and appeal process, the Appellant was dismissed by PWC on 6/10/17 by reason of her conduct at the preliminary hearing and some communications with the Evening Standard about her employment grievances.

6. In the meantime, the Appellant had initiated further employment law proceedings against PWC, to which she subsequently added a claim for unfair dismissal. The hearing of those claims by an employment tribunal took place over 7 days in January 2019. On 12/4/19 the Employment Judge Grewal issued their decision[2] dismissing all of those claims. The Tribunal concluded that the Appellant's behaviour at the hearing was the reason for the dismissal and that the dismissal was fair (paragraphs 136-137). Paragraph 137 summarises the evidence on which the Respondent relies. There is no mention of the incident report completed by the security officer.

7. At the hearing of this appeal the Appellant informed us that she is appealing against the employment tribunal decision relating to her unfair dismissal claim and that that appeal is ongoing.

The subject access requests

8. On 25/10/17, the Appellant sent an information request to the MoJ requesting copies of any CCTV footage, audio recordings and other recorded data relevant to the preliminary hearing on 31/1/17 (page 25). The request was treated as a subject access request ("SAR") under the DPA (page 24). The MOJ responded to that request on 29/12/17 (page 27) and provided her with a copy of the incident report completed by a security officer (page 29-30), which they said was the only relevant information they held. Although that report is dated 31/3/17, the MOJ maintains that it relates to the preliminary hearing on 31/1/17. On 26/4/18 the Appellant complained to the Commissioner about the MOJ's response (pages 57-59) to her SAR. The Commissioner's response and advice dated 6/7/18 is at page 97.

9. At the hearing of this appeal, the Appellant informed us that she was required to provide a copy of the incident report to PWC as part of the disclosure process relating to her ongoing employment tribunal proceedings, and that she did so in around March 2018. She strongly denies the accuracy of that report and its relevance to the preliminary hearing on 31/1/17.

---

[1] https://assets.publishing.service.gov.uk/media/5c3750e4e5274a70e4cfecf6/Ms_Y_Ameyaw_v_Pricewaterhousecoopers_Services_Ltd_2302806-2015_and_others_Judgment.pdf

[2] https://assets.publishing.service.gov.uk/media/5cd542f6e5274a3fd0280ef7/Ms_Y_Ameyaw_-v-_Pricewaterhousecoopers_Services_Limited_-_Case_Number_2200878_2017_-_Full.pdf

The request for information to which this appeal relates

10. On 2/4/18, the Appellant sent a further information request to the MoJ (pages 106-107), framed as a request for *clarification* of their response to her SAR. On that occasion she asked them to provide her with the following further information.

    "1. The name of the officer who prepared the Incident Report dated 31/3/17;

    2. A full list of fixed CCTV camera locations in and around the London South Employment Tribunal at Montague Court, 101 London Rd, Croydon CR0 2RF together with a map of the Tribunal building. Please note that I am referring to cameras in public areas of the Tribunal building that HMCTS operate, or have access to;

    3. A copy of the Court Listing for 31 January 2017;"

11. The MoJ responded on 30/4/18 (page 109). They treated that request as a FOIA request and informed her that they were withholding the part 1 information in reliance on section 40(2) of FOIA and the parts 2 and 3 information in reliance on sections 31(1)(c) and 32(1)(c) of FOIA, respectively.

12. At the internal review stage (page 114), the MoJ upheld their position in all 3 respects.

The complaint to the Information Commissioner

13. The Appellant complained to the Commissioner. We understood that this was by way of a follow up to her complaint about the handling of her SAR, as there is no separate complaint letter in the bundle. In her letter dated 13/12/18 to the Appellant (page 131), the investigating officer made it clear that they were investigating the MOJ's handling of the FOIA request only and they advised her that she needed to let them know if there were other matters that she believed should be added.

14. The MoJ's detailed response to the Commissioner's enquiries (letter dated 31/12/19) is at pages 134-138. As regards part 2 of the request, the MoJ subsequently provided the Appellant with a copy of a floor plan of the public area (page 163) and informed the Commissioner that a list of CCTV cameras did not exist (pages 165-167).

The Information Commissioner's decision

15. On 20/8/19, the Commissioner issued her decision (page 1). She decided that the MoJ -

    - was entitled to withhold the part 1 information in reliance on section 40(2) and the part 3 information in reliance on section 32(1)(c);
    - did not, on the balance of probabilities, hold a list of the fixed CCTV camera locations at the Tribunal venue;
    - in providing the floor plan at a late stage, had breached the FOIA time limits.

The appeal to this Tribunal

16. The Appellant appealed to this tribunal. The outcome she sought was as stated on page 19 ((a) disclosure of the name of the court security officer responsible for completing the wrongly dated incident report; (b) disclosure of the core of her entitlement to access her personal data relating to the alleged incident; and (c) any relief/remedy available to her under the Human Rights Act 1998).

17. Detailed grounds of appeal are given at pages 21A – 21L, under 4 headings.

- **Ground 1** – The Commissioner erred in defining the scope of the investigation and consequently in her approach to the investigation and made no findings on key issues.
- **Ground 2** – The Commissioner erred in law in failing to consider whether the MoJ had properly satisfied the condition listed in section 40(3)(i) of FOIA.
- **Ground 3** – The Commissioner erred in assessing the consequence of disclosure of the court security officer's name.
- **Ground 4** – In carrying out the balancing exercise, the Commissioner failed to properly evaluate the competing rights of the data subject and the public interest. In particular, that the Appellant's Convention rights were engaged and that the data subject was a public official suspected of misconduct.

18. The Commissioner's Response is at pages 88-96 and the Appellant's Reply to that Response is at pages 100-105

The powers of the Tribunal

19. The task of the Tribunal is set out in section 58 of FOIA:

> 58 Determination of appeals
>
> (1) If on an appeal under section 57 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 he ought to have exercised his discretion differently,
>
> the Tribunal shall allow the appeal or substitute such other notice as could have been served by the Commissioner; and in any other case the Tribunal shall dismiss the appeal.
>
> (2) On such an appeal, the Tribunal may review any finding of fact on which the notice in question was based.

The issues we had to decide

20. The only substantive issue we had to decide was whether the Commissioner had correctly concluded that the name of the security guard could be withheld in reliance on section 40(2) of FOIA.

21. We could not consider any issues relating to the SAR decision referred to in paragraph 3 above. There is no right of appeal to this tribunal against a SAR decision.

Relevant law

22. The relevant provisions in section 40 (personal information) of FOIA, as it applied at the date of the Appellant's request, were as follows.

> **40 Personal information**
>
> (1) 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.
>
> (2) 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.
>
> (3) 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 ……
>
> (7) 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.

23. In summary, this means that where a person requests information that consists of another person's personal data, that information is exempt from disclosure under FOIA if its release under FOIA would breach any of the data protection principles. Section 40(2) is an absolute exemption, which means that it is unnecessary for the public authority to undertake the public interest balancing test referred to in section 2(2)(b) of FOIA in order to rely on it.

24. For the purposes of disclosure under FOIA only the *first data protection principle* is of likely relevance:

> Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, [and
>
> (b) ……]

25. In the absence of the consent of the data subject, the only Schedule 2 condition of potential relevance is condition 6(1):

> **6**(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

26. Whether condition 6(1) is met involves the consideration of three questions (paragraph 18 of Lady Hale's judgement in the Supreme Court decision in South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55; [2013] 1 WLR 2421).
    - Is the data controller or the third party or parties to whom the data are disclosed pursuing a legitimate interest or interests?
    - Is the processing involved necessary for the purposes of those interests?
    - Is the processing unwarranted in this case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject?

    In Goldsmith International Business School v Information Commissioner and the Home Office [2014] UKUT 563 (AAC), Upper Tribunal Judge Wikeley set out eight propositions derived from case law as to the approach to answering those three questions (which have come to be known as "the Goldsmith questions").

27. Section 40 was amended by the Data Protection Act 2018 shortly after the date of the request for information (mainly with effect from 25/5/18, when the GDPR[1] became directly applicable). Because the MoJ's review decision (their "last word" in the matter) was not made until 25/9/18, we considered whether the amended version of section 40 (the relevant provisions of which are set out in the Annex to this decision) was the law that the MoJ should have applied at that time. We concluded that the applicable law was that which applied at the date of the *request* for information.

    However, if we were wrong in that respect it would not have changed our decision because the amended provisions are not materially different in the relevant respects to the earlier ones. In reaching that conclusion, we considered, in particular: (a) the definitions of "personal data" and "processing" in the Data Protection Act 2018; and (b) the GDPR "equivalents" of the first data protection principle (Article 5 – Principles relating to processing of personal data - 1 (a) – *personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*) and Schedule 2, condition 6(1) (Article 6 – Lawfulness of processing - (1)(f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*).

The evidence

28. The evidence before us consisted of: the 167 pages of paper evidence in the open bundle of documents that had been produced for the appeal; an

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

unredacted copy of page 136 of the bundle; and the Appellant's oral evidence. We had also been provided with a small bundle of additional open documents comprising Case Management Directions dated 21/1/19 and 31/1/19.

29. During our post-hearing discussions, we were troubled by a possible inconsistency in the timing of key events, as described by the Appellant at the hearing. In particular, we had understood from her oral evidence that she was claiming that it was her disclosure of the incident report to PWC that triggered her dismissal on 6/10/17. However, it was clear that she herself did not receive the incident report from the MOJ until December 2017 (page 27).

    We belatedly noted the Appellant's reference on page 35 to the published decision relating to the strike out application referred to above. The Appellant had not provided a copy of that decision or any case reference, nor did she detail the several hearings relating to her claims before the Employment Tribunal that are summarised in the introduction to this decision. However, a search under her name in the relevant Gov.UK website revealed all three Employment Tribunal decisions referred to above, which provided us with some useful context and background information and clarified the timing of the key events. As we were signposted to one of those decisions by the Appellant's specific reference and they are all publicly available decisions of direct relevance to this appeal, we considered that it was entirely proper for us to consider them before reaching our decision.

The hearing

30. The Appellant requested an oral hearing. The Commissioner had requested a paper determination.

31. The appeal came before us on 20 February in London (Field House). The Appellant attended the hearing. She was unrepresented and ably presented her own case. She was joined part way through by a Mr Ogilvy, her McKenzie Friend.

32. We were somewhat surprised to hear that the Appellant had been expecting us to consider her first information request dated 25/10/17 (page 25) as part of this appeal (particularly (a) as she had expressly said in her Reply to the Commissioner's Response to the appeal that her appeal only concerned the issue of whether section 40(2) applied to the name of the court security officer and (b) because the Commissioner had clearly explained the scope of her investigation in her letter to the Appellant at page 131 and there was no evidence of any objection on her part). However, this appeared to explain her puzzling references at page 19 to ordering "the disclosure of the core of her entitlement to access her personal data" in relation to the alleged incident pursuant to the DPA and her subsequent assertions that the Commissioner had erred in defining the scope of the investigation.

33. We rejected her submissions in that respect. We could not of course consider her first information request because it had (correctly) been dealt with under the DPA as a SAR and therefore fell outside our jurisdiction.

34. The Appellant also objected to the Registrar's directions in paragraphs 6-8 of her Case Management Directions dated 21/1/2 in relation to the information

referred to in paragraph 4.1 and we agreed to consider that point before we made our decision.

What we decided and why

35. Information consisting of the name of the court security officer who completed the incident report was clearly that officer's personal data.

36. We approached the section 40(2) issue from a different angle to the MoJ and the Commissioner. In considering the first data protection principle they started by considering whether disclosure of the name would be fair (and concluded that it would not be fair).

    When *we* considered the first data protection principle, we started by asking ourselves whether any Schedule 2 condition was met (if that was not the case, it would be unnecessary for us to consider the more general question of whether the disclosure would be fair and lawful). This approach was expressly approved by the Upper Tribunal in Farrand v the IC and the London Fire and Emergency Authority [2014] UKUT 0310 (AAC) (paragraph 20 of Judge Jacobs' Decision).

37. There was no suggestion that the security officer had consented to the disclosure and the MoJ was not obliged to seek that consent. The only other potentially applicable Schedule 2 condition was condition 6(1).

Was the Appellant pursuing a legitimate interest or interests?

38. We considered whether, in requesting the court security officer's name, The Appellant was pursuing a legitimate interest or interests (question 1 of the Goldsmith questions).

39. We asked the Appellant to explain her reasons for wanting to know the court security officer's name.

    She cited various public interest reasons for wanting this information. She referred to a general need for accountability/transparency by public officials when undertaking public duties/functions. She said that a public officer should not be able to produce a false report about a court user without identifying themselves. She said that in a situation where serious allegation are made against a member of the public by a public officer who is required to wear an identity badge, that officer should not be permitted to hide behind "a shield of protection" in these sorts of circumstances.

    She also described her own private interests in pursuing this issue; the claimed loss, damage and distress that she asserted had flowed from the misconduct allegations and the possibility of pursuing a remedy against the court security officer concerned (for example, by way of court proceedings against him/her for misfeasance in public office).

40. We asked the Appellant whether she had pursued a complaint to the MoJ about the report and she told us that she had (in September 2019 – with a letter of claim for defamation) but had not yet received any response. She also

told us that she had not applied for rectification of her personal data held by the MoJ as suggested by the Commissioner in the letter at page 97.

41. In considering the relevance of the Appellant's public interest reasons for wanting this information, we took account of the Upper Tribunal decision in Cox v IC and Home Office [2018] UKUT 119 (AAC), where the main issue was whether the general public interest in transparency (and, in particular, the public interest in the disclosure of the names of public officials exercising public functions and powers in the public interest) is *necessarily* a "legitimate interest".

    Judge Wikeley decided that the answer to that question was "no". He said that if that were not the case, it would reverse the position as enshrined in the DPA - with the consequence that "rather than the personal data of public servants being protected unless there are strong reasons to disclose them, instead such personal data would have to be disclosed unless there are strong reasons why it would be wrong to do so".

    He also made the following points:

    - The assumptions about the inherent value and legitimate interest in the disclosure of information that can be taken into account when applying the public interest balancing test under section 2 of FOIA are different to the balancing process in the application of the Goldsmith questions: " ….the section 40(2) exemption applies if disclosure would contravene the data protection principles, so it is the DPA regime which must be applied. There is no obvious reason why the general transparency values underpinning FOIA should automatically create a legitimate interest under the DPA.". (paragraph 42)
    - "The focus of the first stage of the three Goldsmith questions is very much on the legitimate interests of the individual requester and not the more abstract legitimate interests of the public at large." (paragraph 43)
    - "The legitimate interests of an individual requestor may or may not involve the disclosure of officials' names – but that is a context-specific and fact-sensitive question. Such a legitimate interest cannot be automatically assumed."

42. Following the guidance in Cox, we focussed on the Appellant's own legitimate interests in obtaining this information. It is apparent from paragraph 1 of the Employment Tribunal decision referred to in paragraph 6 above that, at the time of her request for information (2/4/18), she was pursuing a claim for unfair dismissal (with other related claims). Subsequently, the Employment Tribunal found that she had been fairly dismissed and the Appellant told us that she is appealing that decision in the Employment Appeal Tribunal (she has not provided any evidence of having been given permission to appeal, but we had no reason to doubt that). At the time of her request she clearly had a legitimate interest in pursuing her unfair dismissal claim.

43. In our judgement, however, there is no plausible reason why the incident report would be relied on as a primary source of evidence or that it would be expected to be comprehensive in relation to incidents of reported misconduct

at the preliminary hearing on 31/1/17. When the issue of the Appellant's conduct at that hearing was considered by Employment Judge Morton in connection with the strike out application (paragraph 3 above) and subsequently by the Employment Tribunal panel in connection with her unfair dismissal claim (paragraph x above) they had the more detailed accounts of Judge Hall-Smith and the other participants who were present at the preliminary hearing to refer to. Like this Tribunal, the Employment Tribunal has case management powers that would, for examples, allow it to require parties and others to provide information to the Tribunal/a party and to require any person to attend any oral hearing as a witness. If she had raised, or was proposing to raise, her concerns about the incident report as part of her unfair dismissal claim, the Employment Tribunal would be in a position to assess the relevance or otherwise of that issue and, if necessary, ascertain the names of any potential witnesses and require their attendance at an oral hearing. The Appellant would not have needed to know the name of the security officer in order to pursue that issue (and indeed she has not claimed that she would).

With reference to paragraph 29 above, either we had misconstrued the Appellant's assertions about the link between the incident report and her dismissal (her dismissal could not have been triggered by her disclosure of the report given that she was dismissed about 5 months prior to that) or the Appellant had simply become confused about dates at the hearing.

44. We considered the Appellant's suggestion that she had a legitimate interest in knowing the name of the security officer so that she could make a legal claim against them personally to be unrealistic and verging on the fanciful. She has alerted the MoJ to her concerns about the report by submitting a complaint to them and is awaiting a response. She does not need the name of the security officer to pursue that complaint with the MoJ.

45. Having decided that the Appellant was *not* pursuing a legitimate interest, it followed that disclosure of the security officer's name would breach the first data protection principle and that that information was, therefore, exempt from disclosure under section 40(2). It was unnecessary for us to consider the second or third questions referred to in the South Lanarkshire case (the necessity test and the possible prejudice to the security officer) or the general issue of fair and lawful processing. For the following reasons, however, we did concur with the Information Commissioner's conclusion that the disclosure of this information would not be fair.

46. The Appellant made assertions about the appointment process for court security officers, which we were not in a position to affirm or deny. She made much of the fact that the court security officer was a public officer, that he/she completed the report in their role as such and should not be permitted to hide behind a "shield" of anonymity given the requirement on security officers to identify themselves as such at work by the wearing of an identity badge (we have no familiarity with such requirements, but considered it highly probable that security officers are required to identify themselves in that way). She asserted that the Commissioner had erred in failing to properly investigate the duties and responsibilities of such an officer.

47. In challenging the Commissioner's conclusion that the security officer would have had a reasonable expectation that the withheld information would not be disclosed to the public at large, it seemed to us that the Appellant had misunderstood the distinction between a public officer who deals with the public and a public officer who is *accountable* to the public.

48. Her appeal documents included a copy of the Commissioner's guidance on *Requests for personal data about public authority employees* (pages 77-83), which says (under the heading *Names in documents): "In assessing whether employees can have a reasonable expectation that their names are not disclosed, key factors include their level of seniority and responsibility and whether they have a public facing role where they represent the authority to the outside world."* It was clear to us that a court security guard does not have the level of seniority and responsibility that would give rise to a reasonable expectation on his/her part that their name in an incident report would be disclosed to the public at large. That is supported by the job advert for a security guard at the Royal Courts of Justice (page 84) which formed part of the Appellant's own evidence. We noted in particular the skills and experience requirements at page 85, which are clearly not commensurate with a senior, publicly accountable public role. A requirement to wear an identity badge whist working is of no relevance to this issue. There are clear and obvious reasons why it would be necessary for a security officer, with some or all of the responsibilities listed at page 84-85, to be clearly identifiable as such to all court users.

49. We also agreed with the Commissioner's conclusions in relation to the second and third limbs of the fairness test. It is clear that the disclosure of the security officer's name to the world at large, in the context of an incident report that he has completed as part of his workplace duties, would be highly likely to cause him unjustified distress. It was also clear to us that his rights and freedoms would trump the Appellant's interests in having that information disclosed to her.

50. The Appellant has made many references to the European Convention of Human Rights. Although Article 8 is engaged here in relation to the security officer, as it is his/her personal data that is at stake, the issue that we had to decide did not involve any potential interference with *the Appellant's* personal data.

51. We considered the authorities referred to by the Appellant, but they were either not relevant to the issue we had to decide, or they did not assist us in deciding that issue.

The case management direction issue

52. With reference to paragraph 49 above, we did not consider it necessary to see the name of the security officer (as contained within an email that does not appear in the open bundle) in order to deal with this appeal fairly and justly.

Conclusion

53. For the reasons given above, we agreed with the Commissioner's conclusion that the release of the security officer's name under FOIA would breach the first data protection principle. The Commissioner's decision notice was, therefore, in accordance with the law and the appeal failed.

Signed: Karen Booth
Judge of the First-tier Tribunal

Date: 2nd May 2020

ANNEX

40 Personal information

(1) 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.

(2) Any information to which a request for information relates is also exempt information if—

(a) it constitutes personal data which [does] not fall within subsection (1), and

(b) [the first, second or third] condition below is satisfied.

[(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under this Act—

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

[(7) In this section—

"the data protection principles" means the principles set out in—

(a) Article 5(1) of the *GDPR* [UK GDPR], and

(b) section 34(1) of the Data Protection Act 2018;

"data subject" has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

"the GDPR", "personal data", "processing" and references to a provision of Chapter 2 of Part 2 of the Data Protection Act 2018 have the same meaning as in Parts 5 to 7 of that Act (see section 3(2), (4), (10), (11) and (14) of that Act)

["personal data" and "processing" have the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2), (4) and (14) of that Act);

"the UK GDPR" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10) and (14) of that Act)].

(8) In determining for the purposes of this section whether the lawfulness principle in Article 5(1)(a) of the *GDPR* [UK GDPR] would be contravened by the disclosure of information, Article 6(1) of the *GDPR* [UK GDPR] (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.]