DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

TO: Mermaids

OF: Main Office, Suite 4, Tarn House, 77 the High Street, Yeadon, Leeds, LS19 7SP; London Office, Office 3, 63 Charterhouse Street, London, EC1M 6HJ

1. Mermaids is Registered Charity Number 1160575.

2. The Information Commissioner ("the Commissioner") has decided to issue Mermaids with a Penalty Notice under section 155 of the Data Protection Act 2018 ("the DPA"). This penalty notice imposes an administrative fine on Mermaids, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 ("the GDPR"). The amount of the monetary penalty is £25,000.

3. This penalty has been issued because of contraventions by Mermaids of Articles 5(1)(f) and 32(1) and (2) of the GDPR in that during the period of 25 May 2018 to 14 June 2019 Mermaids failed to implement an appropriate level of organisational and technical security to its internal email systems, which resulted in documents or emails containing personal data, including in some cases relating to children and / or including in some cases special category data, being searchable and viewable online by third parties through internet search engine results.

In the interests of clarity, 25 May 2018 is the date on which the GDPR became applicable in all member states, including the United Kingdom ("the UK"), and 14 June 2019 is the date on which the controller took steps to secure the email group in question.

4. This Monetary Penalty Notice explains the Commissioner's decision, including the Commissioner's reasons for issuing the penalty and for the amount of the penalty.

Legal framework for this Monetary Penalty Notice

Obligations of the controller

5. Mermaids is a controller for the purposes of the GDPR and the DPA, because it determines the purposes and means of processing of personal data (GDPR Article 4(7)).

6. 'Personal data' is defined by Article 4(1) of the GDPR to mean:

> *information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

7. 'Processing' is defined by Article 4(2) of the GDPR to mean:

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*

8. Article 9 GDPR prohibits the processing of 'special categories of personal data' unless certain conditions are met. The special categories of personal data subject to Article 9 include 'data concerning health or data concerning a natural person's sex life or sexual orientation'.

9. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the GDPR.

10. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure, and to enable them to demonstrate that their processing is secure. Article 5(1)(f) stipulates that:

> *Personal data shall be […] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*

11. Article 32 ("**Security of processing**") provides, in material part:

> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> > *(a) the pseudonymisation and encryption of personal data;*
> >
> > *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*
>
> *2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

The Commissioner's powers of enforcement

12. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the GDPR.

13. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.

14. By Article 58(2)(d) of the GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) she has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.

15. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective, proportionate, and dissuasive in each individual case. Article 83(2) goes on to provide that:

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

> *(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*

16. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner. Section 155 of the DPA ("**Penalty Notices**") provides that:

> *(1) If the Commissioner is satisfied that a person—*
>
> > *(a) has failed or is failing as described in section 149(2) …,*
>
> *the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.*
>
> *(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—*
>
> > *(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR.*

17. The failures identified in section 149(2) DPA 2018 are, insofar as relevant here:

> *(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—*
>
> > *(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
> >
> > *…;*

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors) […]

Factual background to the incident

18. The origins of Mermaids lie in a parents' support group formed by parents whose children were experiencing gender incongruence. It was registered in 1999 with the Charity Commissioner. Mermaids was incorporated as a registered charity in 2015 and offers support to children, young people and their families in relation to gender non-conformity.

19. On 15 August 2016, which is the date on which the email group of relevance to the contraventions set out in this notice was created, the Chief Executive Officer ("the CEO") was at that date the only paid staff member at Mermaids. On 14 June 2019, Mermaids were notified by a service user of the charity that internal emails containing personal data were publicly available online. Mermaids contacted the Commissioner later that day to report the concerns. On 17 June 2019, the CEO telephoned the Commissioner to update her and sent a follow-up email detailing the remedial steps which Mermaids had taken.

Contraventions of Articles 5(1)(f), 32(1) (2) of the GDPR

20. In regard to the principle of integrity and confidentiality under Article (5)(1)(f) of the GDPR, the Commissioner considers that emails were processed by Mermaids on an email group without Mermaids applying the appropriate restricted access settings. If the appropriate security access settings had been applied, then access would have been restricted to approved members of the group only and it would not have been possible for third parties to gain unauthorised access

through the internet to the emails containing personal data, in some cases concerning children and / or in some cases containing special category data, in the period 25 May 2018 to 14 June 2019. In the interests of clarity, 25 May 2018 is the date on which GDPR became applicable in all member states, including the UK, and 14 June 2019 is the date on which the controller took steps to secure the email group in question.

21. In regard to the requirement under Articles 32(1) and (2) of the GDPR to implement a level of security appropriate to the risk when processing data, the Commissioner considers that Mermaids failed to have adequate security measures in place to ensure the appropriate security for personal data in the period 25 May 2018 to 14 June 2019. The email group did not have the appropriate restricted access settings applied to it and therefore the personal data including the special category data were accessible to third parties. Consideration should have been given to pseudonymisation or encryption of the data, either of which would have offered an extra layer of protection to the personal data. Taking such a step may have reduced the opportunity for the emails to be placed at risk in circumstances where Mermaids' organisational memory had failed to account for the existence of the dormant email group after it stopped being used on 21 July 2017. For the avoidance of doubt, the Commissioner has concluded that the nature and gravity of the contraventions are unaffected by the unanswered question as to whether the journalist and third party stumbled across the data by accident or by any possibility, however remote, that individuals deliberately set out to find the information by using a precise and unusual syntactical search. Further, it is considered by the Commissioner that the nature of the contraventions is unaffected by the unanswered question as to the extent to which any other third party or parties accessed the data.

22. The contraventions by Mermaids between 25 May 2018 and 14 June 2019 involved personal data which in some cases included special category data and / or data which was sensitive in its context. The incident involved data which in many cases belonged to children and / or vulnerable individuals. It involved a large group of 550 data subjects and around 24 data subjects whose data was sensitive in its context and / or belonged to children and / or belonged to vulnerable individuals. It has been confirmed in the course of Representations that of those 24 data subjects whose data could be said to be sensitive in context, and / or belonged to children or vulnerable individuals, 15 of the data subjects had special category data accessible. The sensitive nature of the data which was accessible to third parties means that the contraventions necessarily involved significant damage and / or distress to the data subjects, whether or not it was also special category data. The Commissioner has not taken account of any contraventions which may have occurred between 15 August 2016 (i.e., the date of creation of the email group) and 25 May 2018 but has had regard to how the failure first arose and persisted. The Commissioner considers the contraventions to have been negligent.

Notice of Intent

23. On 19 March 2021, in accordance with s.155(5) and paragraphs 2 and 3 of Schedule 16 DPA 2018, the Commissioner issued Mermaids with a Notice of Intent to impose a penalty under s.155 DPA 2018. The Notice of Intent described the circumstances and the nature of the personal data in question, explained the Commissioner's reasons for a proposed penalty, and invited written representations from Mermaids.

24. On 20 April 2021, Mermaids provided written representations in respect of the Notice, together with a supporting document.

25. On 17 May 2021 the Commissioner held a 'representations meeting' to thoroughly consider the representations provided by Mermaids.

Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty

26. The Commissioner has considered the factors set out in Article 83(2) of the GDPR in deciding whether to issue a penalty. For the reasons given below, she is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising her corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

27. In regard to the amount of the penalty, the Commissioner has considered the following facts: Mermaids' total income rose from £317,580 in the year ending 31 March 2018[1], to £715,330 in the year ending 31 March 2019, to £902,440 in the year ending 31 March 2020. The Commissioner is mindful that the penalty must be effective, proportionate and dissuasive.

(a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as

[1] https://register-of-charities.charitycommission.gov.uk/charity-search/-/charity-details/5054976/financial-history

well as the number of data subjects affected, and the level of damage suffered by them

28. **Nature:** The CEO set up an internet-based email group service at https://groups.io, which is overseen by a third party based in the United States of America ("the USA"). In particular, the CEO created GeneralInfo@Groups.IO so that emails could be shared between the CEO and the 12 trustees. An absence of records relating to the creation of the group and the controls that were considered at that time has meant that it has been impossible to establish exactly how the group service was set up, and therefore how the incident originated. The CEO is unable to recall whether the emails were left accessible deliberately to facilitate a general discussion or whether it was an oversight not to select a more secure option and to leave a default security setting in operation. However, after being made aware that the emails were accessible, Mermaids established that the default setting for security and privacy on the Groups.IO internet-based email service provided, "Group listed in directory, publicly viewable messages," which was an insecure and inappropriate setting. Alternative settings available to users of the email service were, "Group not listed in directory, publicly viewable messages,", "Group listed in directory, private messages," and, "Group not listed in directory, private messages," which, if selected, may have provided more appropriately secure settings.

29. The Groups.IO internet-based email group service was in active use by Mermaids from 15 August 2016 to 21 July 2017. After it became dormant it nevertheless continued to hold emails. Mermaids' failure to implement appropriate security settings meant that the email group was listed in the Groups.IO search directory and was indexed on large search engines such as Google. In addition to communications

between the trustees, the emails included some forwarded emails from Mermaids' service users. Mermaids failed to implement an appropriate level of security to its internal email systems, which resulted in documents or emails containing personal data, including in some cases relating to children and / or including in some cases special category data, being searchable and viewable online by third parties through internet search engine results. Mermaids was unaware that it had failed to implement an appropriate level of security or that personal data of its service users was searchable and viewable online by third parties.

30. The last email on the Groups.IO service was sent on 21 July 2017. Nevertheless, the email group remained live and the emails remained publicly visible on the Groups.IO website until remedial actions were taken in June 2019.

31. On 14 June 2019, a service user of the charity, who was the mother of a gender non-conforming child, informed the CEO that she had been called by a journalist from the Sunday Times, who had told her that her personal data could be viewed online. The journalist had informed the parent that by searching online he could view confidential emails, including her child's current name, the child's "dead name", the date of birth, the mother's maiden name and married name, her employer's address, her mobile telephone number and details of her child's mental and physical health. On the same day, Mermaids received pre-publication notice from the Sunday Times that the emails were accessible online and the newspaper would be publishing an article about the incident. Mermaids are understood to have taken immediate steps to block access to the email site before the newspaper report of the incident was published.

32. **Gravity:** The topic of gender incongruence is still regarded, by many commentators and members of the public, to be controversial, and the fact that a child or adult may be experiencing gender incongruence is a sensitive issue which can lead to increased vulnerability. The Commissioner considers that the likely increased vulnerability of a data subject in turn increases the risk of damage or distress being caused to the data subject by any data contravention that reveals that an individual is seeking information about, or support for, gender incongruence. The Commissioner considers that the data about gender incongruence was sensitive in its context. The Government ran a consultation on reform of the Gender Recognition Act 2004 between July and October 2018, which generated widespread public interest in and debate about gender incongruence. Groups supporting transgender rights and people experiencing gender incongruence may be at a higher risk of experiencing prejudice, harassment, physical abuse or hate crime. According to the Home Office Hate Crime report published on 15 October 2019[2], transgender identity is the least commonly recorded hate crime, however, in 2018 it increased by 37%. The large percentage increase may be due to the relatively small number of transgender identity hate crimes of 2,333 during the 2018-2019 period, improvements by the police in identifying and recording such crimes, more people coming forward to report the crimes, or a genuine increase in transgender hate crimes. The Commissioner has had regard to such risks when considering the potential harm that may be caused to affected data subjects.

33. In regard to 15 data subjects, the emails included special category data, such as details of the data subject's mental or physical

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839172/hate-crime-1819-hosb2419.pdf

health and / or sex life and / or sexual orientation, with a further 9 data subjects whose data could be classified as sensitive in context. Four of those 24 data subjects were aged 13 or under in June 2019 and therefore must have been aged 12 or under in the period between 25 May 2018 and 14 June 2019.

34. [redacted]

35. **Duration:** The Commissioner has been unable to confirm the exact duration of the contraventions. However, given the age of some of the data, she is satisfied that it has been occurring, to some extent, since at least 25 May 2018, and she has not considered any contravention prior to this date, which would fall to be considered under the previous data protection regime. The Commissioner considers that Mermaids was in contravention of the GDPR from the date on which it came into force on 25 May 2018 until the issue was remedied by 14 June 2019.

36. **Number of data subjects affected:** The Commissioner understands that around 780 pages of confidential emails were visible online, which included sensitive data relating to gender incongruence and personal data relating to 550 data subjects, such as name, email address, job title, or employer's name.

37. **Damage:** It has not been possible to establish whether or not the data which was exposed online was accessed by third parties other than the Sunday Times journalist. Two data subjects, a mother and a child,

made complaints to Mermaids about the contraventions. The Commissioner also received two complaints.

38. It is reported that 550 emails were accessible and could be viewed online from August 2016 until 14 June 2019. They contained personal data such as names, emails address, job title, employer's name which identified individuals and their connection with the transgender charity. It can be inferred that the individuals whose email addresses were on the group are users of Mermaids, who are a transgender charity, that their data would be sensitive data in context. Most of the email threads contained general discussions, for example, concerning fundraising, arranging attendance at conferences and advice about anti-bullying, and the data subjects were open about their connection with Mermaids. Twenty-four emails have been identified by Mermaids as being of a higher risk, containing more sensitive details within conversations between the CEO, stakeholders and subscribers of Mermaids and included discussions of transgender issues and how the data subjects were feeling and coping with their experiences. Four of these emails related to data subjects who were aged 13 or under as of June 2019. With the introduction of the GDPR, children should be afforded more protection in relation to their data.

39. If someone had accessed the email group online there would have been sufficient available identifying data to potentially "out" the data subject, removing any choice and infringing their privacy.

40. Due to the nature of the services offered by the Mermaids charity, being an organisation who offer support to transgender individuals, the Commissioner expected them to ensure stringent safeguards were in place to protect service users and their personal data. Mermaids received four complaints from former trustees and two from service users. All

complaints have been resolved. [redacted]

(b) the intentional or negligent character of the infringement

41. By 25 May 2018, Mermaids was a well-established significant charity and should have implemented appropriate measures to ensure that personal data was safeguarded, particularly since the data in some cases related to vulnerable children and / or vulnerable adults and / or included special category data and / or a significant proportion of data was sensitive in its context. In the period 25 May 2018 to 14 June 2019, there was a negligent approach towards data protection at Mermaids, data protection policies were inadequate and there was a lack of adequate training, including a lack of face-to-face training, on data protection. Following the introduction of the GDPR, Mermaids' data protection policies had not been updated to ensure compliance. Safeguards should have been in place to protect the young and / or vulnerable data subjects who had used or were using the charity's services, particularly given the probability that personal data controlled or processed by Mermaids would include special category data and / or data which was sensitive in its context.

42. The Commissioner considers that the contraventions were not deliberate, although there is an element of negligence as the CEO created the email group with the least secure settings in error. This was compounded by the fact the CEO, not nor any other person associated with the charity, did not correctly close down the email group, thereby leaving it accessible, albeit dormant.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

43. As soon as Mermaids were made aware, by the service user, that the email group was accessible, the charity immediately took the email group down and took proportionate action to ensure any data collected was removed from any archive website.

44. [redacted]

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

45. All Mermaids staff and volunteers received mandatory data protection training in December 2018, which is updated annually, however, the ongoing contraventions were not identified by anyone at Mermaids during the period of operation of the insecure email system, which demonstrates that the training was inadequate and / or ineffective.

46. The CEO of Mermaids created the email group with the least secure settings. Even though it was created in 2016 which would have been covered by the Data Protection Act 1998, the group remained live and accessible until June 2019, with the same settings that were applied on its creation in 2016. The settings were the least secure and allowed access to the email group and the contents of the emails were

viewable online. When the use of the email group ceased there was no clear documentation to demonstrate how it was created or decommissioned. The email group remained dormant but accessible and appears to have been forgotten.

47. In addition to the change in data protection legislation such as the introduction of the GDPR, the Government consultation concerning the Gender Recognition Act 2004 ("GRA") and associated public debate on gender incongruence should have prompted Mermaids to re-visit their policies and procedures to ensure appropriate measures were in place to protect individuals' privacy rights.

(e) any relevant previous infringements by the controller or processor

48. The Commissioner is unaware of any previous data protection infringements by Mermaids.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adve effects of the infringement

49. Mermaids were co-operative and replied to the enquiries promptly. They employed both solicitors and a data protection consultant to review the incident and to oversee any remedial action. Mermaids also instructed a specialist media law firm on 14 June 2019. They received four complaints from former trustees and two from service users – all of which have been concluded.

50. Mermaids immediately adjusted the settings on the Groups.IO website so that the data was no longer accessible to third parties.

Mermaids staff began reviewing all the emails which had been exposed to viewing by third parties. Mermaids also reported itself to the Commissioner on 14 June 2019.

51. On 15 June 2019, [redacted] The same day, the Sunday Times printed an online article stating that 1,000 pages of confidential emails by Mermaids were available on the IO platform which had been active between 2016 and 2017 and could be viewable online. The same day, Mermaids informed an initial number of data subjects, whom it regarded as "sensitive data subjects", and for whom Mermaids had contact details, about the incident. Also on 15 June 2019, Mermaids published a press statement on its website which included an apology. Also on 15 June 2019, Mermaids notified the Charity Commission of the existence of a serious risk incident. Also on 15 June 2019, Mermaids liaised with Groups.IO to obtain metadata to identify when the relevant data had been accessed by third parties and Mermaids were told by Groups.IO that they did not collect that metadata.

52. On 16 June 2019, a printed article was published in the hard copy Sunday Times, drawing attention to the matter. Also on 16 June 2019, Mermaids notified all former trustees and major funders of the incident; and took initial steps to transition its email service to a more secure email platform.

53. On 17 June 2019, Mermaids engaged a data protection consultant. Also on 17 June 2019, Mermaids updated the Charity Commission about the incident.

54. On 18 June 2019, Mermaids learnt that various archived or cached versions of the data remained online, and therefore their solicitors requested Google to remove them, and the data were immediately removed. Similar steps were taken by Mermaids to remove data from Archive.li. The same day, Mermaids sent the Commissioner an update.

55. On 19 June 2019, Mermaids liaised with Groups.IO to request information regarding users making requests of the Mermaids' group's archives. Three further data subjects were identified by Mermaids as "sensitive data subjects". Mermaids continued its efforts to remove access to the data via Archive.li.

56. On 20 June 2019, the three additional "sensitive data subjects" were notified of the incident. Legal advisors to Mermaids reviewed with staff the current data systems at Mermaids for any further areas of vulnerability. The same day, Mermaids instructed their solicitors to begin liaising with the "sensitive data subjects".

57. On 21 June 2019, Groups.IO confirmed that they did not hold any relevant information in their logs. The same day, Mermaids engaged an information technology security auditor, to begin to review the incident on 27 June 2019. [redacted]

58. On 22 June 2019, [redacted] confirmed that the data had been removed. Mermaids' solicitors contacted all the "sensitive data subjects" to explain the remedial steps which had been taken and provided copies of their data which had been affected. They also sought permission from the data subjects whose data had been uploaded on Archive.li to contact Archive.li on their behalf to seek [redacted]

59. Between 24 June 2019 and 25 June 2019, the law firm obtained all the consents required from the data subjects to remove the data from Archive.li and sent compliance notices to Archive.li and its webhost, copied to their local data protection authorities. Mermaids held a trustee meeting to provide an update to trustees on the remedial steps which had been taken to address the contraventions, with Mermaids' external legal advisers in attendance.

60. On 26 June 2019, Mermaids updated their website message to include reference to Archive.li.

61. On 27 June 2019, two additional "sensitive data subjects" were identified by Mermaids, they were updated on the remedial steps which had been taken and they were sent copies of the personal data which had been exposed. On the same day, Mermaids was alerted to the fact that a larger group of data subjects had been affected by the incident. On Mermaids' instruction, the solicitors then reviewed all the data which had been accessible online to ensure all remedial actions had been taken. Mermaids, through their lawyers, notified the Commissioner and also chased the Sunday Times for a substantive response to their letter of 21 June 2019.

62. On 28 June 2019, Mermaids' solicitors updated the "sensitive data subjects" whose data had been uploaded to Archive.li to confirm that the relevant webpages had been removed. They also sent an update to the Commissioner; continued to review the data; wrote seeking further information from Groups.IO, if available, about the extent of any third-party access to the data in question; and updated the Commissioner on what remedial actions had been taken.

63. On 25 July 2019, the CEO completed half a day of data protection training from an external trainer, in response to the contraventions.

64. The Commissioner understands that the specialist data consultant appointed by Mermaids completed a review of all Mermaids' data systems and policies to ensure they were compliant with the GDPR and that Mermaids undertook to implement all his recommendations. The Commissioner understands that the contravention has been identified as an isolated incident and no wider issues were identified during the review. Further, it appears that all policies at Mermaids have now been updated to conform to the GDPR and that Mermaids undertook to put all data protection policies on one place on the intranet where they would be easily accessible to all staff and volunteers. Further, a security assessment was undertaken by a specialist consultancy, over a three-week period in June to July 2019, involving a review of all systems and processes at Mermaids to assess security and access controls, recommendations were made, implementation was agreed and the recommendations were then implemented by Mermaids to strengthen security and privacy.

(g) the categories of personal data affected by the infringement

65. These include information allowing identification of individuals, including children; in some cases the data was sensitive in context relating to gender incongruence, and in some cases it was special category data, including data relating to health.

66. The email addresses identified 550 data subjects, all of whom had been in contact with Mermaids at some point. Due to the nature of the services offered by Mermaids it can be inferred that some of data of those individuals can be identified as special category data. 24 have been identified by Mermaids as being of a higher risk, containing more sensitive details with conversations between the CEO, stakeholders and subscribers of Mermaids and included discussions around transgender issues and how the data subjects were feeling and coping with their experiences. 15 of those 24 data subjects had special category data accessible. Some of the emails show an exchange with Tavistock and Portman NHS Foundation Trust, who run a gender identity clinic. These emails disclose health information. 4 of those 24 data subjects were under 13 as of June 2019.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

67. Mermaids notified the Commissioner about the infringement on 14 June 2019. [redacted]

[redacted] Mermaids reported themselves to the Commissioner on the same day.

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

68. Not applicable.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

69. Not applicable.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

70. An aggravating factor is the duration of the infringement from 2017 to 2019.

71. Since 2016, Mermaids has raised its profile and in recent years it has received funding from various sources, including from the National Lottery, Children in Need and the Government. These factors have contributed to an increase in the public attention which Mermaids receives and the good standing from which it has benefited. Regulatory action against Mermaids will serve as an important

deterrent to other entities or persons who are not complying or who are risking not complying with their duties under the GDPR.

72. The Commissioner has taken account of the prompt remedial actions taken by Mermaids in response to becoming aware of the incident, which reduced the detriments caused to the data subjects, and of Mermaids' co-operation with the Commissioner.

73. Mermaids' profile significantly increased after being linked to a television programme. This breach was highlighted in a national newspaper and that resulted in a degree of reputational damage to the charity. The Commissioner considers that whilst the fine itself should act as a deterrent, it was important to balance this against ensuring the charity is able to maintain effective provisions for service users nor taking away donations made by the public.

Summary and decided penalty

74. For the reasons set out above, the Commissioner has decided to impose a financial penalty on Mermaids. The Commissioner has taken into account the size of Mermaids and the financial information which is available about the charity on the Charity Commission website, as well as the representations that Mermaids has made to her about its financial position. She is mindful that the penalty must be effective, proportionate and dissuasive.

75. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on Mermaids of **£25,000** (**twenty-five thousand pounds**).

Payment of the penalty

76. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **3 August 2021** at the latest. The 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.

77. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) The imposition of the penalty; and/or,
(b) The amount of the penalty specified in the penalty notice

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

79. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired

80. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the 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.

81. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA 2018.

Dated the 5th day of July 2021

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

ANNEX 1

Rights of appeal against decisions of the commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a 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

   Telephone: 0203 936 8963
   Email: grc@justice.gov.uk

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 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 (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20))