6.2 Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

6.3 If the data breach is unlikely to result in a risk to the rights and freedoms of those affected by the breach, then the notification to the ICO described at 6.1 will not be necessary.

6.4 A data breach is likely to result in a risk to the rights and freedoms of those affected by the breach if it causes a loss of control over their personal information or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality. These examples are not exhaustive, and the breach must be assessed on a case-by-case basis by the DPO.

6.5 If a notification to the ICO is made, the DPO will ensure that appropriate steps are taken to fully co-operate with their requests / investigations.

7. Notifying the Data Subject(s)

7.1 Subject to 7.2, if the data breach is likely to result in a high risk to the rights and freedoms of the data subject(s) the DPO will ensure that steps are taken by the Trust to notify the data subjects without delay using the letter template at appendix 2.

7.2 Those affected by the data breach need not be notified if any of the following apply:-

(a) The Trust had implemented appropriate technical and organisational measures, and those measures were applied to the personal information affected by the data breach, in particular, those that ensure the personal information is unintelligible to any person who is not authorised to access it, such as encryption and the data is recoverable e.g. as it was backed-up.

(b) The Trust has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

8. Post Breach Procedure

8.1 It is imperative that regardless of how serious or minor the breach, lessons are learnt, and measures are put in place to avoid a similar incident occurring again in the future. The DPO will be responsible for making any necessary recommendations to improve data protection practices.

8.2 The measures put in place should be proportionate to the breach; however, such measures could include the provision of further training, introduction of new policies and procedures or changes to security measures.

APPENDIX 1

The Information Commissioner's Office
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[Date]

Dear Sirs,

Notification of a Data Breach in accordance with Article 33 of the General Data Protection Regulation ("GDPR")

We write to the Information Commissioner's Office in accordance with Article 33 of the GDPR to provide notification of a data breach. It is considered that the breach is notifiable on the basis that it is likely to result in a risk to the rights and freedoms of those affected.

[We are aware that notification should be made to the ICO by no later than 72 hours after having becohm0 g3(free)-3(d)14(o)] TBT-2.92 reW*nBT/F1 11.04 Tf1 0 0 1 72.024 396.89 Tu1 pr(rig)7(hf1 0 595.32 841.da)-2

The likely consequences of the data breach

[INW*h7 50.*

N)5(W*h7 50.*tUI

APPENDIX 2

[Name]
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]
[Date]

Dear XXXX

Notification of a Data Breach

We write to advise you of a recent data breach within the Trust. Having considered the nature of the breach, we have reported this to the Information Commissioner's Office who will advise us of the next steps in their process. The ICO is the UK's independent body set up to uphold information rights.

DPO@wearehy.com

The likely consequences of the data breach