ICO Ref: **COM0570983**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Anxiety UK

Zion Community Resource Centre
339 Stretford Road
Hulme
Manchester
M15 4ZY

I, Nicky Lidbetter, Chief Executive, of Anxiety UK, for and on behalf of Anxiety UK hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Anxiety UK is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by Anxiety UK and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. In February 2015 the Information Commissioner (the 'Commissioner') was informed by Anxiety UK that personal data held within a password protected area of Anxiety UK's website, was publically available for approximately 12 months via an internet search engine. It was determined that the information was cached due to a coding error. Personal data including the names, addresses, email addresses and anxiety condition of members who had agreed to share their information with other members of Anxiety UK only, was made available on the internet as a result.

3. Whilst there was a contract in place between Anxiety UK and the third party company appointed to build the website, the data protection provisions were extremely limited. The Commissioner's investigation revealed that the data controller had failed to ensure that the data processor had sufficient technical measures in place to properly secure its systems. For example, appropriate penetration tests were not conducted prior to the website launch. Had this been done it is likely that the code error would have been detected prior to the launch of the website.

4. In addition, it appears that out of date membership details were available on the website. The Commissioner's investigation therefore determined that the data controller's quality assurance controls were inadequate. In particular, there was a lack of robust review mechanisms in place.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of this matter. The relevant provisions of the Act are the fifth and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data compromised in this incident consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

6. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the fifth & Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

1) **The data controller shall implement appropriate periodic security testing of its website; the scope of this testing should be determined by the risks to the personal data processed on its site;**

2) **The data controller shall implement adequate contractual controls and supporting review mechanisms to ensure that data processors acting on their behalf achieve and maintain compliance with the requirements of the seventh principle;**

3) **The data controller shall implement appropriate retention, review and disposal controls to ensure that personal data is not held for longer than is necessary in compliance with the fifth principle;**

4) **The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Signed: ……

Nicky Lidbetter
Chief Executive
Anxiety UK

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….