ICO Ref: **ENF0385229**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Child Exploitation and Online Protection Centre
Serious Organised Crime Agency
PO Box 8000
London
SE11 5EN

I, Peter Davies, Chief Executive Officer of the Child Exploitation and Online Protection Centre ("CEOP"); and I, Trevor Pearce QPM, Director General of the Serious Organised Crime Agency ("SOCA"), for and on behalf of SOCA, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Serious Organised Crime Agency 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 CEOP on behalf of SOCA. 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. On 6 April 2011, the Information Commissioner (the "Commissioner") received a complaint from a member of the public about the security of the online reporting form on CEOP's website. On 13 April, CEOP also contacted the Commissioner to confirm the organisation was aware of the matter.

3. On 1 April 2011, the complainant had accessed CEOP's online form to make a confidential and sensitive report. On doing so, they discovered that the website's reporting page was insecure, meaning that any information would be transmitted over the internet in an unencrypted format in clear text. Investigations revealed that this had been the case for several months, and the fault had not been identified either during initial testing of the new website, or in the following months. Several other website security weaknesses subsequently came to light.

4. In deciding what action to take, the Commissioner has considered that, whilst the reporting forms generally contain sensitive personal data, there is no evidence that any of the information has been intercepted. Further, each page of the form is sent separately to servers that host the CEOP website, at which stage the pages are then combined and encrypted. The Commissioner has also noted that although the problem lay undetected for several months, as soon as the issue was identified, a fix was implemented, and all pages are now submitted in an encrypted format.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data potentially compromised in this incident may have included "sensitive personal data" as defined under section 2 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1. Regular checks are carried out on the data controller's websites to ensure that they remain secure, and that any potential weaknesses are immediately identified;

2. All recommendations in the data controller's Information Security Review report are fully implemented by 31 August 2011 and are subsequently monitored;

3. Any third party website contractors are fully aware of their requirements and responsibilities in ensuring that personal data is held and transmitted securely. These responsibilities will be reflected in appropriate contracts between the parties;

4. The data controller shall implement such other security measures as it deems appropriate to ensure that personal

data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Dated…….

Signed……
Peter Davies
Chief Executive Officer
Child Exploitation and Online Protection Centre

Dated…….

Signed……..
Trevor Pearce QPM
Director General
Serious Organised Crime Agency

Signed……
Sally Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner