DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: **Scottish Children's Reporter Administration**

Ochil House
Springkerse Business Park
Stirling
FK7 7XE

I, Neil Hunter, Chief Executive of Scottish Children's Reporter Administration for and on behalf of Scottish Children's Reporter Administration hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Scottish Children's Reporter Administration 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 Scottish Children's Reporter Administration 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. The data controller informed the Information Commissioner (the "Commissioner") of two data security incidents.

3. The first incident involved the emailing to an unknown third party of draft submissions which contained sensitive information relating to a child's court hearing under the Children (Scotland) Act 1995.

4. During the court proceedings, the sheriff ordered that draft submissions be exchanged between relevant parties. The employee of the data controller provided their home email address to receive the submissions. It was then attempted to forward the documents concerned to the line manager's home email address however, the email was wrongly addressed and they were sent to an unknown third party. This was done despite the data controller's policy that states documents may only be transmitted by email if they are to another organisation of equivalent security.

5. The second incident involved the temporary loss of nine case files containing sensitive personal data relating to the safety and welfare of children. The files were contained in a cabinet which was removed from the data controller's premises as part of a temporary office decant. The cabinet, containing the case files, was subsequently sold in a second hand shop. The files were later retrieved by the data controller.

6. It was the data controller's understanding that the contractor conducting the decant would destroy the cabinets. Prior to the decant, employees of the data controller had been given relevant training and were told that they were responsible for ensuring that files were removed from cabinets. As a result of data controller employees failing to follow instructions and confusion about the role of the contractor, the case files left the premises in an unsecure manner.

7. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of these matters. 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 in both incidents 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 of the Act.

8. 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) Staff are aware of the data controller's policy for the storage and use of personal data, in particular, that they are not permitted to email personal data to a private email address, and are appropriately trained how to follow that policy;

(2) Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;

(3) During office moves, the data controller will ensure, in addition to staff being made aware of relevant policies and procedures, that steps are taken to check that these are being followed;

(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 process, accidental loss, destruction, and/or damage.

Dated…….

Signed……

Neil Hunter
Chief Executive
Scottish Children's Reporter Administration

Signed……

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