DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Gwent Police

Croesyceiliog
Cwmbran
Torfaen
NP44 2XJ

I, Mick Giannasi, Chief Constable of the Gwent Police for and on behalf of Gwent Police hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Gwent Police 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 the Gwent Police 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 April 2010 the Information Commissioner (the "Commissioner") was provided with a report by Gwent Police which recorded the circumstances of a data security breach concerning Criminal Record Bureau (CRB) enquiries performed by the Force.

3. On 15 February 2010 a member of the IT staff with the Gwent Police forwarded an email intending that it be received by five police staff colleagues. The email was inadvertently copied to a web site journalist, whose address had been auto suggested in the cc field of the email as the journalist shared a name with one of the intended addressees.

4. The email in question contained a Microsoft Excel spreadsheet as an attachment containing some 10,000 CRB enquiry results, which had been requested by the Gwent Police. 863 of these records indicated the individual concerned had some degree of information recorded. The record did not disclose the nature of the information, and in particular did not disclose details of any criminal convictions recorded.

5. Subsequently an internal investigation discovered that the member of staff responsible for circulating the email in question had also demonstrated a somewhat caviller attitude in respect of Gwent Police IT security policy in relation to the use of passwords, disclosure on a needs to know basis, the volume of data transferred (given the purpose of the transfer) and the management of suspected corrupt files.

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 disclosed in this incident consisted of information relating to an individual's involvement in the commission, or alleged commission, of an offence. Personal data containing such information is defined as "sensitive personal data" under section 2(e) of the Act.

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. Physical and technological security measures are adequate to prevent unauthorised access to personal data;

2. Technological measures are introduced, and maintained, which will prevent inappropriate auto completion of addresses in internal and external email accounts.

3. Technological measures are introduced, and maintained, which will enforce restricted marking on documents intended for transmission by email.

4. Where a business need exists to access sensitive personal data such access should be provided via direct and secure access to the appropriate data base. Only when such an option is not available will sensitive personal data be transferred by secure email account, and then only the data required for the specific purpose of the transfer will be transmitted.

5. The use of 'Generic passwords' is prohibited.

6. Staff are made aware of the data controller's policy in respect of the restrictions placed on the emailing of sensitive personal data.

7. 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……

Mick Giannasi
Chief Constable
Gwent Police

Signed……

Mick Gorrill
Assistant Commissioner, Enforcement Division
For and on behalf of the Information Commissioner