DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: The University of York

Heslington
York
YO10 5DD

I, Professor Brian Cantor, Vice Chancellor of The University of York, for and on behalf of The University of York hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The University of York 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 University of York 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. On 17 March 2011, the Information Commissioner (the 'Commissioner') received correspondence from the data controller, stating that personal data relating to a number of University students had been compromised via a University website. The personal data in question included the name, address and date of birth of the students, together with certain course details.

3. In September 2009, the data controller undertook a software development project, in order to update a University web template. A test programme was created which was not appropriately secured. Once completed, the application in question was moved to its proper place on the data controller's live web server, but the test version was not deleted. This test version remained available to unauthorised users and gave access to information from the live student database.

4. Due to a lack of management control and change management processes within IT Services, the data controller failed to identify risks posed by their actions, which subsequently resulted in the error not being detected for a considerable period.

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.

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) University IT staff must ensure the appropriate security of all such data following any system maintenance conducted, prior to the system being restored for general use;

(2) Remote access to any University IT systems, that store or process personal data, must be subject to appropriate security;

(3) Appropriate penetration and vulnerability testing is performed annually in respect of all University IT systems that store or process personal data;

(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.

Signed: ……

Professor Brian Cantor
Vice Chancellor
The University of York

Dated: …….

Signed: ……

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

Dated: …….