ICO Ref: **COM0562205**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: King's College London

Strand
London
WC2R 2LS

I, Professor Edward Byrne AC, President & Principal, of King's College London, for and on behalf of King's College London hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. King's College London 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 King's College London 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 Information Commissioner (the 'Commissioner') was informed by the data controller that a spreadsheet containing personal data, including exam results, of 1831 students and applicants was sent in error to 22 students. The spreadsheet was being used to assign coursework titles and associated instructions for a module, however the relevant information was not extracted from the spreadsheet and it was sent out in its original form. The spreadsheet had been worked on by and transferred between several employees of the data controller prior to being sent out in error. No formal checking process was in place and it was not recognised that irrelevant personal data was contained on the spreadsheet being sent out.

3. Whilst the data controller was able to contain the breach it was evident that insufficient organisational measures were in place to prevent the disclosure of personal data in this incident. By way of enquiries it was established that there was an absence of written supporting procedures for staff to follow around sending personal data to students. There was also a lack of mandatory data protection training in place at the data controller. Data protection training was available on demand

but only 461 of approximately 6000 staff (7.7%) had taken this during the year prior to the incident and records relating to training completion were not stored centrally. The data controller stated that they intend to roll out a system of mandatory data protection training which all staff will be required to complete every two years, however it was not anticipated that all staff will have received this training until October 2016.

4. 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.

5. 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) The data controller shall introduce mandatory DPA training for all staff handling personal data by 31 October 2015. The data controller shall require its employees to receive this training on induction and for this training to be refreshed at least every two years.

(2) The data controller shall ensure that all staff handling personal data receive the above data protection training by 31 December 2015.

(3) The data controller shall ensure that completion of data protection training sessions is fully monitored and that completion statistics are reported to relevant senior management and/or working groups, e.g. the SIRO or an information governance group. Appropriate follow up procedures should also be in place in the event of staff non-compliance.

(4) The data controller shall review its policies to ensure

that appropriate checking procedures are in place when sending communications to students and that there are written procedures or guidance to support these by 30 September 2015.

(5) 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: ……

Professor Edward Byrne AC
President & Principal
King's College London

Dated: …….

Signed: ……

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

Dated: …….