

DATA INCIDENT – JUNE 2017

Outcome of Information Commissioner's Investigation

The Information Commissioner (ICO) has investigated the circumstances surrounding the emailing error which led to sensitive data on a number of students being circulated to a student group email address. After careful consideration the ICO has decided not to take enforcement action on this occasion given the facts of the case and the remedial measures that have already been taken by the University, which the ICO expects to be implemented University-wide, to prevent any recurrence.

The ICO has emphasised the importance of a number of steps that the University is taking to improve compliance with the Data Protection Act and added further detail. The University must ensure that all staff receive data protection and related training on induction, staff should positively acknowledge that they have read and understood appropriate policies and procedures, the uptake of initial and refresher training should be carefully monitored and there should be clarity as to the consequences if the appropriate training is not completed. The University should review policies and processes in the light of this particular incident, and with particular emphasis on the use of internal and external email. Further incidents could result in enforcement action (which can include substantial fines), particularly if the University fails to take steps to reduce the risk of a recurrence.

Notwithstanding the ICO's decision that regulatory or enforcement action is not appropriate to this case, the ICO has made a number of observations concerning the application of the seventh data protection principle, that technical and organisational measures should be taken to avoid the unauthorised processing of (in this case sensitive) personal data. The spreadsheet containing sensitive personal data was circulated within the University without password protection and not all staff involved had received training on the requirements of the Data Protection Act. More generally the levels of completion of data protection training in the University have been poor and there have been other email-related incidents (albeit with lesser impact) where lessons could have been learned related to the risk of using email for transmitting personal data.

The importance of implementing the University's action plan, which will be updated to reflect the detail of the ICO's recommendations, cannot be overstated.