APPENDIX 1

DATA BREACH REPORT FORM

Section 1: Notification of Data Security Breach **To be completed by Head of Dept. of person reporting incident**	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and contact details of person reporting incident (email, address, telephone number):	
Brief description of incident or details of the information lost:	
Number of people affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Investigating Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity

To be completed by the Investigating Officer with the Head of Dept. of the area affected by the breach and IT where applicable

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special category 'sensitive' personal data** (as defined in the relevant data protection law(s)) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) genetic or biometric data; f) commission or alleged commission of any offence, or g) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. • Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; • Personal information relating to vulnerable adults and children;	

• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Spreadsheets of marks or grades obtained by students, information about individual cases of student disciplinary or sensitive negotiations.	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken **To be completed by Data Protection Officer and/or Investigating Officer**	
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and/or Investigating Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Investigating Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on: Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**