



DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department, complete Section 1 of this form and email it to the Data Protection Officer (DPO) and IT Help desk where appropriate.

Section 1: Notification of Data Security Breach To be completed by Head of department of person reporting incident	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects 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:	
<i>For use by the Data Protection Officer</i>	
<i>Received by:</i>	
<i>On (date):</i>	
<i>Forwarded for action to:</i>	
<i>On (date):</i>	

Section 2: Assessment of Severity

To be completed by the DPO in consultation with the Head of area affected by the breach and if appropriate 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?	
How many data subjects are affected? Is the data bound by any contractual security arrangements?	
<p>What is the nature of the sensitivity of the data?</p> <p><i>Please provide details of any types of information that fall into any of the following categories:</i></p>	
<ul style="list-style-type: none"> • HIGH RISK personal data: special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's <ul style="list-style-type: none"> a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation 	
<ul style="list-style-type: none"> • 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; 	
<ul style="list-style-type: none"> • Personal information relating to vulnerable adults and children; 	

<ul style="list-style-type: none"> 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; 	
<ul style="list-style-type: none"> Security information that would compromise the safety of individuals if disclosed. 	

Section 3: Action taken

To be completed by the DPO

ID Incident number	
Report received by:	
On (date):	
Action taken by officer/s responsible :	
Was incident reported to authority?	Yes / No If Yes, notified on (date):
Follow up action required/recommended:	
Reported to the DPO on (date):	
Reported to other internal stakeholders (details, dates):	

For use of Data Protection Officer

Notification to National Information Technology Development Agency (NITDA)	Yes / No If Yes, notified on (date): Details:
Notification to data subjects	Yes / No If Yes, notified on (date): Details:
Notification to other external, regulator / stakeholder	Yes / No If Yes, notified on (date): Details: