UFORM022 Personal Data Breach Report Form Rev 1

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your line manager immediately. Line managers need to complete Section 1 of this form and email it to the DPO at dpo@unihaven.ie.

Section 1: Notification of Data Security Breach	To be completed by Line Manager of the person reporting the 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, etc.):	
Brief description of incident or details of the information lost:	
The 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:	

For college use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by DPO in consultation with the Line Manager affected by the breach.
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 college or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g., to student sponsors?	
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 o Sensitive personal data (as defined in the Data Protection Acts) 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) commission or alleged commission of any offence. f) 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.	
o Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas.	
o 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 discipline or sensitive negotiations which could adversely affect individuals.	
○ Security information that would compromise the safety of individuals if disclosed.	
Category of the incident (Lo Risk, Risk, Hi Risk):	
Reported to CEO:	
If Risk or Hi Risk, date escalated by DPO to the CEO/Executive Management Team	
Signature: _____	Date: _____