

4.2 Personal Data Security Breach Report Form

As a matter of urgency when a Personal Data security breach has occurred please complete this form and return it to the Information Governance Officer at foi@dit.ie and your Line Manger.

The requirement in Stage 4 above that all incidents in which personal data has been put at risk must be reported to the ODPC within 2 days of DIT becoming aware of the incident is relevant here.

1.	Details of the data breach	
2.	Date and time incident occurred	
3.	Date and time incident detected	
4.	What type of data is involved?	
5.	Does data fall under the definitions of personal data and / or sensitive personal data outlined in Section 3?	
6.	Details on how the personal data was held (e.g. laptop, memory stick, personal digital assistant etc.)	
7.	Details of safeguards if any that would mitigate the risk if personal data has been lost or stolen. (e.g. encryption)	
8.	Are there any reasons to suspect that the passwords used to protect the personal data may have been compromised? (e.g. password stored with mobile device or weak password used)	
9.	Details of the number of individuals whose personal data is at risk (i.e. how many data subjects are affected by the breach?)	
10.	Details of those whose personal data has been breached (e.g. staff, students, suppliers or third parties)	
11.	Details of what the personal data could tell a third party about the data subjects affected	
12.	Any other relevant information or details that you consider relevant	

Signed:
(Name of person reporting incident)

Date: