Contents

Purpose........................................................................................................................................1
Obligations....................................................................................................................................1
Purpose

Under the Data Protection Acts 1988 and 2003 Dublin City University, as a Data Controller, is obliged to process personal data entrusted to the University in a manner that respects the rights of data subjects to have their data processed fairly. DCU is specifically obliged to take appropriate measures to protect the security of such data.

This document addresses Data Breach situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. A Data Breach does not just relate to lost USB keys/disks/laptops. It may also include any loss of control over personal data entrusted to DCU, including inappropriate access to personal data on university systems or the sending of personal data to the wrong individual(s).

Obligations

A Data Breach, i.e. the loss of control of personal data in manual or electronic form, must be reported immediately to DCU’s Data Protection Officer, who will give immediate consideration to the required next steps. In most situations DCU are required to make a report to the Office of the Data Protection Commissioner within two days of the breach occurring.

Personal data stored on an encrypted laptop with secure access controls is not considered by the Data Protection Commissioner to involve a risk. However, it should be noted that the strongest encryption software is useless if the access password is stored with the device, or if the password is weak.

In a situation where a third party is processing data on behalf of DCU the data processor must notify DCU as soon as they become aware of the incident. This duty should be reflected in appropriate contracts between DCU and any third party data processor.

DCU’s Data Protection Officer will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data.
More information can be found on the Data Protection Commissioners 
website.