1.6 Personal Data Security Breach Management

A Personal Data security breach ("data breach" in short) occurs when Personal Data is made available to one or more third parties without the consent of the data subject. Data breaches may occur in a variety of contexts, e.g.:

- Loss or theft of data (e.g. on a memory stick, laptop or paper records)
- Inappropriate access controls (e.g. using unsecure passwords)
- Equipment failure
- Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
- Disclosing confidential data to unauthorised individuals
- Human error (e.g. emails being sent to the wrong recipient)
- Hacking, viruses or other security attacks on IT equipment systems or networks
- Breaches of physical security (e.g. forcing of doors/windows/filing cabinets).

If you consider that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing **Personal Data Security Breach Report Form** in Section 4.2. Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

It is much better to report a data protection breach straight away than to "cover it up" and risk negative consequences down the line. A data protection breach is not a disciplinary issue, and once the breach has been reported the Information Governance Officer will handle things from there.

There is a requirement that all incidents in which personal data has been put at risk must be reported to the Data Protection Commissioner within 2 days of DIT becoming aware of the incident.

Subsequent to each data security breach a log will also be maintained by the Information Governance Officer of the agreed steps arising from each incident and this will be presented by way of an overall annual report to the President or his nominated Committee.

Further Information is available in Section 4.1.