Data Protection
Procedural Guidelines for Personal Data Security Breaches
1 Introduction

Trinity College Dublin is obliged under Data Protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a personal data security breach. It is vital to take prompt action on foot of any such actual, potential or suspected security breach to avoid the risk of harm to individuals, damage to operational business and financial, legal and reputational costs to the University.

The purpose of these guidelines is to supplement College Data Protection Policy by providing a framework for reporting and managing security breaches involving personal or sensitive personal data. These guidelines may be used by all members of the College community in a combined effort to minimise the damage done by personal data security breaches.

2 What is a personal data security breach?

A personal data security breach is any incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data held by the University.

Personal data security breaches may occur in a variety of contexts, such as:

- Loss or theft of data, equipment on which data is stored (e.g. a memory stick) or paper records
- Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords)
- Equipment failure
- Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account)
- Disclosing confidential data to unauthorised individuals
- Collection of personal data by unauthorised individuals
- Human error/accidental disclosure of data (e.g. emails containing personal or sensitive information 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 there is any doubt as to whether a personal data security breach has occurred, the Information Compliance Officer should be consulted immediately.

These guidelines apply to all personal data created or received by the College in any format, including data that is accessed remotely. Personal data is defined as information relating to a living individual who is or can be identified either from the data or from the
data in conjunction with other information that is in, or is likely to come into, the possession of the College.


3 Procedure for reporting personal data security breaches

Any personal data security breach must be dealt with immediately and appropriately.

If a member of the College becomes aware of an actual, potential or suspected breach of data security, he/she must report the incident to the Information Compliance Officer immediately.

After reporting the incident, he/she must complete the Personal Data Security Breach Report form and email it to the Information Compliance Officer as soon as possible.

4 Procedure for managing personal data security breaches

Upon receiving notification of a personal data security breach, the Information Compliance Officer shall, in conjunction with any appropriate members of staff, take the following steps (in line with best practice) when responding to the breach.

4.1 Step 1: Identification & initial assessment of the incident

If any member of the College considers that any data security breach has, or might have, occurred, they must report this breach immediately to the Information Compliance Officer and complete the Personal Data Security Breach Report form.

The Personal Data Security Breach Report form will assist the Information Compliance Officer in conducting an initial assessment of the incident. This assessment will take into account:

- Whether a personal data security breach has taken place
- The nature of the personal data involved in the breach (i.e. whether sensitive personal data is involved)
- The cause of the breach
- The extent of the breach (i.e. the number of individuals affected)

---

1 ‘Guidance on data security breach management’ (2012), Version 2.1, UK Information Commissioner’s Office
• The potential harms to which affected individuals may be exposed
• Any steps that may be taken to contain the breach

Following this initial assessment of the incident, the Information Compliance Officer may, according to the severity of the incident, consult with the College Secretary and decide if it is necessary to appoint a group of relevant College stakeholders (e.g. IS Services, Human Resources) to assist with the investigation and containment process.

4.2 Step 2: Containment & Recovery

In the event of a personal data security breach, immediate and appropriate steps must be taken to limit the extent of the breach.

The Information Compliance officer, in consultation with any relevant College staff, will:
• Establish who within the College needs to be made aware of the breach (e.g. IS Services, Communications office) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network)
• Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach
• Where appropriate, inform the Gardaí (e.g. in cases involving criminal activity)

4.3 Step 3: Risk Assessment

The Information Compliance Officer, in conjunction with any relevant College staff, will use the information provided in the Personal Data Security Breach Report form to fulfil the requirement to consider the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

An assessment of the risks for the College, including strategic and operational, legal, financial and reputational risks may also be prepared.

4.4 Step 4: Notification

In accordance with the Data Protection Commissioner’s “Personal Data Security Code of Practice”\(^2\), all incidents in which personal data has been put at risk must be reported to the ODPC within 2 working days of the College becoming aware of the incident.

Incidents do not have to be reported to the Officer of the Data Protection Commissioner when:

\(^2\) Approved July 2011.
• The full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and  
• The incident affects no more than 100 data subjects and  
• The incident does not affect sensitive personal data or personal data of a financial nature.

All contact with the Data Protection Commissioner should be made through the Information Compliance Officer.

The decision to report a breach to the ODPC will ultimately be made by the College Secretary, in consultation with the Information Compliance Officer and any relevant College staff. If a decision is made not to report a breach, a brief summary record of the incident with an explanation of the basis for not informing the Office of the Data Protection Commissioner will be retained by the Information Compliance Officer.

4.5 Step 5: Evaluation & Response

In the aftermath of a personal data security breach, a review of the incident may take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise.

5 Further Information

Further information can be obtained from the College Data Protection policies and procedures, the website of the Office of the Data Protection Commissioner and the Information Compliance Officer.

Trinity College Data Protection Website: http://www.tcd.ie/info_compliance/dp/  
Staff Contact Information: http://www.tcd.ie/info_compliance/dp/contact.php