IT Services Process for Lost or Stolen IT Devices Version 1.1

Process Owner:	IT Services
Process Manager:	Ms Karen Jago: User Support Manager
Version:	1.1
Date:	26 May 2021
Created By:	Gerard Fitzsimons
Signed Off By:	Ms Karen Jago: User Support Manager
Proposed Revision Date:	26 May 2022

Step 1: A Theft is Reported
A user reports the theft of a University owned IT device.

Step 2: A Ticket is opened and assigned to User Support
The ticket will be opened and assigned to a User Support advisor.
The Request Type shall be set security Incident.

Step 3: Information Gathering
The advisor to whom the ticket is assigned shall work to answer the following questions by engaging with the user, engaging with the relevant department and consulting the asset register in ServiceDesk.

- When the incident occurred.
- Where the incident occurred.
- What device(s) is/are involved.
- If a theft, is there a police report.
- Is the device encrypted?
- Is Personally Identifiable Information (PII) affected by this incident?

Step 4: Information Security
If the device was encrypted, proceed directly to Step 5.
If the device was not encrypted and Personally Identifiable Information is involved the incident will be passed to the Information Security Manager.

Step 5: Ordering a Replacement Device
A separate ticket will be opened and assigned to the User Support Team to deal with ordering a replacement device.
The user must be advised from the outset that they or their department may have to bear the cost of this.
The excess on the University Property Insurance is currently €5000. Users must advise the University Health & Safety Officer in advance if they plan to travel in order to be covered by University Travel Insurance Policy.

Step 6: Notifying Original Supplier of Theft/Loss
Where a Dell device has been reported lost or stolen and a police report exists for this, the User Support Advisor will notify Dell of the incident. On receipt of a copy of the police report, Dell will cancel all future support for that device.

Step 7: Closure of Original Ticket.
If the incident has not been passed to the Information Security Manager at Step 4, the original ticket, opened in Step 2, can be closed once Steps 1 to 6 are completed.