Information Security Incident Response Policy

1. Introduction

service Self Service Desk, and do not require the completion of a Security Incident Reporting Form.

4. Roles & Responsibilities

4.1 All users of University Information are responsible for reporting information security incidents. This includes actual, potential, and suspected incidents.

4.2 Heads of School and Functions and Line Managers are responsible for ensuring all users of University information are made aware of this policy, and for assisting with any investigations or incident management response as required.

4.3 The University Secretary has overall responsibility for Information Management and ensuring effective governance of Information Management policies, procedures and training.

4.4 The IMPS Officer (Lead Officer for IMPS) is responsible for: the communication and management of Information Security Incident reports; maintaining a central record of incidents reported and actions taken; advising on mitigations, changes to current practices and making best practice recommendations; co-ordination of incidents referred to the Information Security Incident Team (ISIT), and advising on and completing notifications to the Information Commissioners Office (ICO).

4.5 The Director and Assistant Director (s) of DTS (Lead Officer for DTS) are responsible for assessing Information Security Incident reports referred to DTS, dealing appropriately with those incidents that do not require further escalation, and notifying

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
0.1		IMPS	JAN 17	UEB	JAN 17	APRIL 17	APRIL 18
0.2	No changes	IMPS	APRIL 19	UEB	APRIL 19		APRIL 20
0.3	IT Services amended to DTS	IMPS	May 20		April 20		April 21