

Annex A: Map of Documents within the University Information Security Framework (elements with  fill are in *draft*)

Information Security Framework							
	Data Protection	Cyber Threats	Physical Threats	Freedom of Information	Corporate Records	Intellectual Property and Copyright	Allied Activities
Regulation (Mandatory)	Regulation 31 governing the use of computing facilities					Regulation 28 covering intellectual property rights	
Policy (Mandatory)	Data Protection Policy University Records Management Policy				Research Data Management Policy University Records Management Policy		Risk Management Policy Open Access Policy Security Policy
Practices/Procedures (Mandatory or Recommended)	Working Practices for Protecting Electronic Information Information Classification and Handling Procedure Report an Incident Procedure CCTV Manual Regulation of Investigatory Powers Act Statement			FoI Publication Scheme			Research Code of Practice ITS Specific Procedures covering specific technical areas / roles (e.g. use of software, email, connection to campus network, system administrators code of practice)
Guidance (Advisory)	Information Security Workbook for Procurement of Software or Services involving UoW Information Guidance on Use and Selection of Cloud Service Providers			Freedom of Information Act Guidelines	Guidance on Email Management	Copyright Guidelines	Business Continuity and Emergency Planning