UNIT	**ICT**	**Information and Communications Technology**				
IT-01	**Information and Communications Technology: Strategy and Planning**					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward/Data Manager**
ICT Strategy	Until superseded	Permanent	Archive	Industry Standard	Internal	CIO
ICT Strategy - Draft Files	Publication date	5 years	Destroy	Industry Standard	Internal	CIO
ICT Projects	Duration of project	5 years	Destroy	Industry Standard	Internal	CIO
Service Level Agreements	After the terms of the agreement/contract have expired	5 years	Destroy	Statute of Limitation	Internal	CIO
Submissions - Business cases for approval	Duration of project	5 years	Destroy	Industry Standard	Internal	CIO
IT-02	**Information and Communications Technology: Operations**					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward/Data Manager**
Staff Accounts and Data	Lifetime of Account Use	6 months	Destroy	Industry Standard	Confidential	CIO
Student Accounts and Data	Lifetime of Account Use	2 years	Destroy	Industry Standard	Confidential	CIO
Applications Development and Administration	Lifetime of Application Use	5 years	Archive	Industry Standard	Confidential	CIO
IT Service Management	From task closure	3 years	Destroy	Industry Standard	Internal	CIO
Minor administrative records	Current year	5 years	Destroy	Industry Standard	Internal	CIO
Network and System Logs	Current Year	1 year	Destroy	Industry Standard	Internal	CIO
Third Party Network Access Requests	Termination of Connection	3 years	Destroy	Industry Standard	Internal	CIO
Departmental File Share/Doc Management Information	Current year	5 years	Destroy	Industry Standard	Internal	CIO

Technical Reports	Current year	5 years	Destroy	Industry Standard	Confidential	CIO
IT-03	**Information and Communications Technology: Hardware and Software**					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward/Data Manager**
IT Asset Management	Disposal of asset	5 years	Destroy	Industry Standard	Internal	CIO
Back-ups (VIP User Data)	Current backup	2 years	Destroy	Industry Standard	Confidential	CIO
Back-ups (User Data)	Current backup	90 days	Destroy	Industry Standard	Confidential	CIO
Back-ups (System Data)	Current backup	3 years	Destroy	Industry Standard	Confidential	CIO
Manuals, Service Catalogues and operating procedures	After system no longer used	5 years	Destroy	Industry Standard	Internal	CIO
Policies and Procedures	Until superseded	5 years	Destroy	Industry Standard	Internal	CIO
Information Security Management (incident responses and investigations)	After date created	5 years	Destroy	Industry Standard	Confidential	CIO
Software Licences	Lifetime of software	5 years	Destroy	Industry Standard	Internal	CIO
Warranty	Lifetime of warranty	5 years	Destroy	Industry Standard	Internal	CIO
IT-04	**Information and Communications Technology: Data Protection and Security**					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward/Data Manager**
Detection and investigation of security breaches of an ICT system, and action taken	Last action on incident	5 years	Destroy	Industry Standard	Confidential	CIO
Protective Monitoring Server Reports	From date of report	5 years	Destroy	Industry Standard	Confidential	CIO

Standalone audit reports	From date of report	5 years	Destroy	Industry Standard	Internal	CIO
IT-05	**Information and Communications Technology: Business Continuity and Risk Management**					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward/Data Manager**
Business Continuity Planning (BCP)	Until superseded	Permanent	Archive	Industry Standard	Confidential	CIO
BCP – Training Programme Development	Date superseded	5 years	Destroy	Industry Standard	Internal	CIO
BCP – Training Programme Delivery	Date superseded	5 years	Destroy	Industry Standard	Internal	CIO

Record	The record type	***Data Classification**	**Description**
Trigger	Event that prompts the start of retention period	Public Data	May be viewed by all members of TU Dublin and the public. Data should be classified as Public when the disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Such data is often made available to the public via the TU Dublin website. This data will not cause harm to any individual, group, or to the University if made public.
Retention Period	Period for which the records should be retained	Internal Data	Information that can be used and shared within TU Dublin but would not be appropriate to be known to people outside the University. This data could be released to the public under Freedom of Information legislation
Action	The action to be taken when the non-current period has expired	Confidential Data	Accessible only to relevant members of staff of TU Dublin or designated third parties who require it to perform their duties.
Rationale	The basis on which the Action is recommended		

Data Classification	The security classification category assigned to the records (see across) *		
Data Steward/Data Manager	The title of the officeholder primarily responsible for the records and for ensuring implementation of the RRS in respect of those records. The job title should be entered rather than individual name, preferable as personnel may change over time.		

Date Approved by Head of Function	14/07/2025
Date Reviewed by Information Governance Office	27/08/2025
Date of Last Review	14/07/2025