UNIT	CPVA	Child Protection and Vulnerable Adults				
01	Child Protection and Vulnerable Adults					
Records	**Trigger**	**Retention Period**	**Action**	**Rationale**	**Data Classification**	**Data Steward**
Child protection/welfare concern records	Case Closure	10 years (longer if ongoing risk/litigation)	Destroy	Legal risk, duty of care, GDPR proportionality	Confidential	Mandated person, DLP/DDLP
Safeguarding concerns (low-level, not escalated)	Case closure	7 years	Destroy		Confidential	Mandated person, DLP/DDLP, Designated Area Leads
Referrals to Tusla / HSE	Case closure	Align with main case file	Destroy	Ensures complete case record	Confidential	Mandated person, DLP/DDLP
Reports made to An Garda Síochána (if applicable)	Case closure	Align with main case file	Destroy	Ensures complete case record	Confidential	Mandated person, DLP/DDLP
Retrospective disclosures (e.g. historical abuse)	Scenario 1 – U18 still at risk	10 years (longer if ongoing risk/litigation)	Destroy	GDPR minimisation; retain only if actionable	Confidential	Mandated persons
	Scenario 2 – U18 not still as risk	7 years	Destroy	GDPR minimisation; retain only if actionable	Confidential	Mandated persons
Anonymous disclosures / reports	Date received	2–5 years (unless linked to case)	Delete	GDPR minimisation; retain only if actionable	Confidential	Mandated person, DLP/DDLP
Safeguarding disclosures (informal notes)	Case closure or incorporation into formal file	Retain with case file	Merge into official record	Avoid duplication, ensure single source of truth	Confidential	Mandated person, DLP/DDLP, Designated Area Leads
Internal referrals and escalation decisions		7 years (longer if ongoing risk/litigation)	Destroy	GDPR minimisation; retain only if actionable	Confidential	Mandated person, DLP/DDLP, Designated Area Leads
Case management notes	Case closure	Align with case file	Secure delete / archive	Completeness of safeguarding record	Confidential	Mandated person,

						DLP/DDLP, Designated Area Leads
Safeguarding risk assessments	Superseded	7 years	Archive then delete	Evidence of compliance and risk management	Internal	Designated Area Leads, Chair CPVA Committee, CRO
Correspondence (referrals, acknowledgements, feedback) with external agencies (Tusla, Gardaí, HSE)	Case closure	Align with case file	Secure delete / archive	Completeness of safeguarding record	Confidential	Mandated person, DLP/DDLP
Internal communications related to safeguarding decisions		7 years (longer if ongoing risk/litigation)	Archive then Delete	GDPR minimisation; retain only if actionable	Confidential	Mandated person, DLP/DDLP, Designated Area Leads
Safeguarding logs/registers (concerns tracking)	Last entry	7–10 years	Secure delete	Oversight and trend analysis	Confidential	Mandated person, DLP/DDLP, Chair of CPVA committee
Audit review findings related to safeguarding cases	Audit	Indefinite (to ensure audit record history)	Archive	Corporate governance, audit, inspection evidence	Internal	Chair CPVA committee and Information Governance Officer
Safeguarding training records (staff)	Training completion	5–7 years	Secure delete	Demonstrates compliance with Children First obligations	Internal	Head of People Development
Safeguarding policies & procedures	Superseded	Permanent	Archive	Corporate governance, audit, inspection evidence	Public	Chair of CPVA Committee

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 Manager	Any member of staff with operational responsibilities in the day-to-day data administration activities including, but not limited to, developing, maintaining, distributing and securing institutional data. Data managers are expected to have high-level knowledge and expertise in the content of data within their area of responsibility.		

Date Approved by Head of Function	29 June 2026
Date Reviewed by Information Governance Office	02 July 2026
Date of Last Review	02 July 2026 (new)