Dublin City University

Data Retention Policy

Version Control Panel

Document Name: DCU Data Retention Policy
Owner: Data Protection Unit - Office of the Chief Operations Officer
Approved by: DCU Executive
Review frequency: Every 5 years

Version	Description of Changes	Approval Date
V1.0	Approval in full of the policy by the DCU Executive	15 May 2018

1. **Overall Objective / Purpose**

This is the data and document Retention Policy ("**Retention Policy**") of Dublin City University ("**DCU**"). This Policy applies to DCU, which includes each of the DCU Campus Companies as listed in the DCU Privacy Policy and all staff, employees, officers and contractors engaged by DCU (together "**DCU Personnel**"). The purpose of this Retention Policy is to state DCU's policy concerning the retention and destruction of Personal Data (e.g. documents, records, emails and correspondence, files, audio visual files and recordings and any other forms of information and records regardless of their format together referred to as "**Data**").

2. **Retention principles**

Having regard to the principles contained in Article 5(1) of the General Data Protection Regulation (EU No. 2016/679) ("**GDPR**"), it is the policy of DCU to:

(a) retain personal data in identifiable form only for such period as is necessary in relation to the purpose for which the data are processed (the "**storage limitation**" principle);

(b) ensure that personal data retained by DCU is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed (the "**data minimisation**" principle); and

(c) take all reasonable measures to ensure that personal data retained by DCU are accurate (the "**accuracy**" principle).

3. **DCU Statutory Functions**

3.1 Having regard to Article 24 of the GDPR, the storage limitation, data minimisation and accuracy principles must be considered in light of the nature, scope, context, purposes and the risks arising in the context of the data processing undertaken by DCU pursuant to its important statutory objects and functions as provided for under the University Act, 1997 (as amended) (the "**University Act**").

3.2 While sections 12 and 13 of the University Act state the general objects to be pursued and functions to be performed by DCU, section 13(1) specifically states that it is the function of a university to "*do all things necessary and expedient in accordance with* [the University Act] *to further the objects and development of the university"*, which together are referred to as the "**DCU Statutory Functions**".

3.3 In performing its tasks in the public interest when discharging DCU Statutory Functions, DCU therefore has a lawful basis to undertake data processing, including the retention of personal data. Accordingly, it is the policy of DCU to retain and hold personal data in performing DCU Statutory Functions in a manner that is consistent with the principles of storage limitation, data minimisation and accuracy.

5. **Application of this Retention Policy**

5.1 This Retention Policy applies to any type of Data created, received, transmitted and retained in the context of DCU's day to day activities in performance of DCU Statutory Functions and any other data processing undertaken by DCU, regardless of the format.

5.2 Therefore, any paper records or electronic files that are part of any of the categories listed in a unit specific Personal Data Security Schedule ("**PDSS**"), must be retained

for the period indicated in the PDSS. Data should not be retained beyond the period indicated in the PDSS, unless a valid operational reason (or a litigation hold or other exceptional situation) calls for its continued retention. If you are unsure whether to retain a certain record, in the first instance please contact your local Data Protection Champion. A Data Protection Champion may escalate the query where appropriate to the DCU Data Protection Officer (DPO) (email - data.protection@dcu.ie).

6. Data Ownership

All Data, irrespective of format, generated, created, received and/or retained by DCU in performing the DCU Statutory Functions is the property of the University and subject to its overall control. DCU Personnel leaving DCU or changing positions within DCU are not to remove any Data without the prior written authorisation of their Department/Unit Head.

7. How to store Data

7.1 DCU's records must be stored in a safe, secure and accessible manner to ensure the security and confidentiality of such Data in accordance with DCU's Data Privacy Policy and DCU's '*Information & Communications Technology (ICT) Security Policy*', which is available at: ISS Policies

7.2 Special care is to be taken to ensure that information of a sensitive nature, in particular, information that constitutes a special category of personal data under the GDPR,[1] is stored in a secure manner which may include, for example, locked filing cabinets and offices for hard copy Data and/or the use of password protection and encrypted files for Data stored in electronic form.

8. How to Destroy Data

8.1 Once Data have met their required retention period under the applicable PDSS, in accordance with the principles set out in this Retention Policy, such Data should then be transferred to the DCU approved archives or deleted or destroyed or anonymized as follows:

(a) ***Hard copy files***: to be destroyed by confidential shredding or by using the services of an approved confidential waste disposal firm.

(b) ***Electronic files***: to be purged or deleted or anonymized from all relevant systems on which such Data is stored and/or data bases.

(c) ***Data stored in other media***: to be deleted or destroyed or anonymized in a safe and confidential manner to ensure the content is not disclosed.

9. Litigation Holds and other scenarios

9.1 What is a Litigation Hold?

DCU requires all DCU Personnel to fully comply with the general guidance set out in this Retention Policy and the specific retention periods set out in each unit specific PDSS. However, all DCU Personnel should note the following general exception to any stated destruction schedule: if you believe, or the DCU Chief Operations Office

[1] **Comment**: Such data includes: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

and/or the HR Department informs you, that certain Data held by DCU is relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change such Data, including e-mails, until the DCU Chief Operations Office and/or the HR determines that such Data is no longer needed. This exception is referred to as a "**Litigation Hold**", and takes priority over any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the DCU Chief Operations Office and/or the HR Department

9.2 **What to do when notified of a Litigation Hold?**

The destruction of Data must stop immediately upon notification from DCU Chief Operations Office and/or the HR Department that a litigation hold is to begin due to ongoing or potential litigation or an official investigation. Destruction may begin again once DCU Chief Operations Office and/or the HR Department, as appropriate, has confirmed that the relevant litigation hold has been lifted.

10. Compliance with this Policy and Questions

10.1 It is the responsibility of each DCU Department/Unit to ensure that personal data is retained by that Department/Unit in compliance with this Retention Policy and to ensure that all DCU Personnel under their responsibility comply with this Retention Policy. Operational responsibility rests with each Executive Dean(s) and Director(s)/Head(s) of central administration of each Unit.

10.2 To facilitate compliance with this Retention Policy, each DCU Department/Unit is required to maintain a PDSS which contains information of the various personal data retained by that Department/Unit.

10.3 Each DCU Department/Unit shall maintain an up to date PDSS, which is to be reviewed and updated by the Department/Unit on an annual basis. The updated PDSS shall be provided to the DCU Data Protection Officer (DPO), email – data.protection@dcu.ie

10.4 For guidance on compiling the PDSS please refer to the document: 'Guidance to preparing and using DCU Personal Data Security Schedule (PDSS)', which is available at the following link: guide. A PDSS template is available at the following link: template.

10.5 Any questions about this Retention Policy, or how to compile the PDSS, should be referred in the first instance to your Data Protection Champion, who may escalate matters to the DCU DPO, as appropriate.

End.