Data Retention Policy

Document Owner:	Data Protection Officer
Classification:	Data Protection
Document Identifier:	Data Retention Policy
Internal/External use:	Internal and external
Approval:	Policy Management Group
Document Status:	Approved
Version:	1.0
Date Issued:	9 May 2018
Last Review:	14 March 2024
Last Modified:	25 March 2024
Next Review:	25 March 2025

Data Retention Policy

Printed copy of this document is uncontrolled and should not be relied upon as the most up to date version.

Table of Contents

Scope

This policy applies to Trinity College London (together with its wholly owned subsidiaries, "**Trinity**", "**us**", "**our**" or "**we**"), and to:

- all Trinity employees, workers and trustees;
- all consultants, contractors, agency or temporary workers and other service providers engaged by Trinity where the contract between Trinity and such party specifies that they are to comply with Trinity's policies and procedures.

This policy applies to the retention of personal data, which is processed and subsequently retained by Trinity. It should be read in conjunction with the Data Retention Schedule which specifies retention periods for each type of personal data. This policy applies to personal data held on all Trinity systems, whether hosted on site or in the cloud, on portable storage media or devices, on our own servers, third party servers, email accounts, backup storage such as photographic, microform and electronic media that are used to store records as well as to more traditional paper or card records.

For employees, the contents of this policy are not contractual. It is the responsibility of everyone to familiarise themselves with this policy and comply with it.

Trinity reserves the right to amend this policy without notice.

Aims of the Policy

This policy addresses the requirements in relation to data retention under the GDPR [1] and sets out how Trinity meets its obligations under the law and to individuals regarding the retention of personal data. Personal data should only be retained for as long as there is a real operational, business or regulatory requirement to retain it.

The purpose of this policy is to:

- minimise the retention period of records while ensuring that the information, operational, business and regulatory needs and requirements of Trinity are met;
- ensure that records required for legal and evidential purposes are kept for the appropriate period and in an appropriate manner; and
- ensure that records are not destroyed prematurely.

We need to follow this policy in order to:

- ensure that Trinity complies with the law;
- protect the rights of the data subjects whose personal data we process; and
- protect Trinity, its staff, and other associated persons.

Commitment

Trinity is committed to setting out and ensuring the observance of the regulatory requirements for the proper retention of personal data.

[1] In this policy, 'GDPR' refers to the General Data Protection Regulation ((EU) 2016/679) and Regulation (EU) 2016/679 as it forms part of the law of England, Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments) etc (EU Exit) Regulations 2019 (as amended).

Roles and Responsibilities

The Data Protection Officer ("**DPO**") has overall responsibility for the operation of this policy and is responsible for ensuring that this policy is reviewed in line with operational and GDPR requirements.

All directors and managers (and designated project leaders, where applicable) are responsible for ensuring adherence to this policy within their teams.

Implementation Requirements

- Trinity shall not keep personal data for longer than is necessary for a given purpose. No personal data should be kept indefinitely 'just in case'. However, the retention period can differ based on the type of data processed.

- The Data Retention Schedule lists the types of personal data maintained by Trinity and specifies the retention period for each data type. Trinity should periodically review the data we hold, and where Trinity acquires a new type of personal data, Trinity's DPO should be notified and the Data Retention Schedule must be updated accordingly.

- Where there is a statutory retention period for a record, this will be treated as a minimum period.

- After the retention period has expired, the personal data should be destroyed in accordance with Trinity's Data Destruction Policy. Personal data does not necessarily have to be completely erased. In line with Trinity's Data Destruction Policy it is sufficient to anonymise the data, for example, by erasing single pieces of information that identify the data subject (whether alone or in combination with other pieces of information). In cases where the data cannot be allocated to an identifiable person, no action will be required.

- No records involved in any investigation, litigation or audit will be destroyed until legal counsel has confirmed that no further legal reason exists for retention of the record. It is the responsibility of senior management involved to ensure related documents have been segregated appropriately.

- In terms of transparency and information obligations, data subjects must be informed of:
  - the retention period;
  - if no fixed retention period can be provided – the criteria used to determine that period; and
  - the new retention period if the purpose of processing has changed after personal data has been obtained.

- A document should not normally be stored both on paper and electronically, nor stored electronically in several different locations; a single electronic version (stored so as to be accessible to all who need the information it contains) is preferred. There may be some exceptions to this, for example, exam-related paperwork referring to candidate enrolments, results and/or reports where we may take a scanned copy for ease of access to the information but where we also need to keep the original for purpose of checking signature or other hand-written details.

Consequences of non-compliance

The ICO can issue an enforcement notice against Trinity where it fails to comply with the law. This could have monetary and reputational repercussions for Trinity.

Failure to retain personal data in accordance with this policy can also have other negative ramifications for Trinity, including regulatory investigations, fines and penalties, negative customer perception, reputational damage, loss of information and costs associated with notifying concerned parties of data loss and/or inadvertent disclosure. Therefore, it is imperative that all staff familiarise themselves with the contents of this policy and follow its requirements. Any questions about personal data retention should be referred to the DPO (dpo@trinitycollege.com) or, where the question involves the technical system requirements relating to such retention, to IT Services.

All staff should be aware that any breach of data protection legislation may result in Trinity's disciplinary procedures or termination proceedings being instigated, as appropriate.

Training

Trinity will carry out training for the appropriate teams in relation to this policy. This is in addition to the mandatory data protection training that all Trinity staff are required to complete on a schedule determined by Trinity.

Related documents: This policy should be read in conjunction with Trinity's:

- Data Protection Policy;
- Data Destruction Policy;
- Data Retention Schedule;
- Trinity's other policies related to data protection and IT security located on the intranet under the Resources section, including (but not limited to) Trinity's Data Protection by Design and by Default Policy, Data Protection Impact Assessment Procedure, Data Breach/Loss Response and Notification Procedure, Data Subject Rights Policy and Procedure, Data Transfer and Sharing Policy, Cookie Policy and Information Security Policy; and
- Trinity's privacy statement as well as privacy statements relating to specific groups of data subjects such as Trinity's employee privacy statement available on the intranet under the Resources section.

Other references: The ICO's website has detailed guidance in relation to data retention which can be found here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/

Change Control

Change History

The following changes have been made to this document:

Version	Date	Author	Change Summary
0.1	16 Mar 2018	Compliance Manager	Policy updated to incorporate GDPR requirements
0.2	08 May 2018	Compliance Manager	Further updated to incorporate GDPR requirements

0.3	07 March 2023	Data Protection Officer	Amended to refer to GDPR being incorporated into UK law
1.0	14 March 2023	Data Protection Officer	Refreshed the wording and brought into an up-to-date format.

Change Approval

The changes to this document have been approved by the following personnel:

Version	Date	Approver
0.2	23 May 2018	Trinity's Executive
1.0	25.03.24	Policy Management Group