Data Destruction Policy

Document Owner:	Data Protection Officer
Classification:	Data Protection
Document Identifier:	Data Destruction 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 Destruction 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 3

Aims of the Policy 3

Commitment 3

Roles and Responsibilities 3

Implementation Requirements 4

Consequences of non-compliance 5

Training 6

Change Control 6

- Change History 6
- Change Approval 6

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 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

Trinity is aware of its obligations under the GDPR[1] to retain personal data in a safe and secure manner for only as long as is necessary and then to properly dispose of such personal data. This obligation applies whether the personal data is in a paper-based or electronic format.

This Data Destruction Policy outlines Trinity's approach to fulfilling this obligation to dispose of personal data when it is no longer required, and is closely aligned with Trinity's Data Retention Policy and Data Retention Schedule.

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 requirements for proper disposal of paper-based and electronic personal data.

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.

[1] In this policy, 'GDPR' refers to that 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).

Implementation Requirements

Trinity is aware of its obligations under the GDPR to retain personal data in a safe and secure manner for as long as is necessary and then to properly dispose of personal data whether it is in paper-based or electronic format.

Paper files, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Trinity data, some of which is considered both commercially and personally sensitive. In order to protect the data, all storage media must be properly disposed of. Electronic media should also be 'wiped' prior to being appropriately destroyed, to remove any risk that confidential or sensitive data remains retrievable.

However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, where required, special tools must be used to securely erase data prior to equipment disposal.

Manual or Paper-based Data Disposal

Personal data which is contained in manual or paper-based records should be disposed of in accordance with the Data Destruction Procedure and in keeping with the principles as set out below:

1. Trinity will schedule a regular review of its retention of paper-based records and will identify those that will need to be destroyed and those where it will be 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);

2. Trinity will schedule timely destruction of paper-based records where retention has exceeded Trinity's operational requirements and regulatory obligations as captured in Trinity's Data Retention Schedule;

3. these records will be collected and stored in a secure environment prior to destruction;

4. Trinity will make confidential waste bins available within the organisation in order to dispose of paper records which have no, or short-term, retention periods – this may include (but is not limited to) general office correspondence, hand-written notes used prior to transcription, copies of documents which might have been used for short-term cross-reference, etc.

5. staff will be trained and made aware of their obligation to shred material using in-house shredders;

6. for the bulk disposal of paper records for which there is a medium- to long-term retention obligation, Trinity may appoint an appropriately specialised third party to process the act of destruction of these records, using approved and recognised industry standard methods;

7. the third party will be required to sign an appropriate data processing contract, as per GDPR requirements and to provide a certificate of secure destruction on request; and

8. to minimise the risk of inadvertent loss or disclosure, all manual records due for destruction should be shredded as soon as possible once their retention has exceeded the respective retention obligation.

Technology Equipment Disposal

Technological equipment containing personal data should be disposed of in accordance with the Data Destruction Procedure and in keeping with the principles as set out below:

1. Trinity will schedule a regular collection of end-of-life technology equipment, throughout the organisation. This equipment will be collected and stored in a secure environment, prior to destruction;

2. Technology equipment in the scope of this policy includes:
   - Internal Hard Drives (Physical/SSD);
   - External hard Drives (Physical/SSD);
   - RAM Modules;
   - Tapes (DAT/DLT/LTO);
   - CD/DVD/Blu-ray;
   - Mobile Phones/PDAs; and
   - USB Sticks;

3. where required, Trinity will appoint an appropriate third party to process the act of destruction of this equipment, using approved and recognised industry standard methods; and

4. the third party will be required to sign an appropriate data processing contract, as per GDPR requirements.

Personal data in electronic records

Personal data which is contained in electronic records should be disposed of in accordance with the Data Destruction Procedure.

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 properly dispose of personal data in accordance with this policy and the related Data Destruction Procedure 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 disposal 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 scheduled determined by Trinity.

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

- Data Destruction Procedure;
- Data Retention Policy;
- Data Retention Schedule;
- Data Protection Policy;
- 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 the destruction of personal data 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/#no_longer_need

Change Control

Change History

The following changes have been made to this document:

Version	Date	Author	Change Summary
0.1	09 May 2018	Compliance Manager	Policy first drafted
0.2	20 Feb 2020	Compliance Manager	Policy updated
0.3	7 March 2023	Data Protection Officer	Policy updated
1.0			The Data Destruction Policy was separated out into a separate policy and procedure in accordance with the new template formats.

Change Approval

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

Version	Date	Approver
1.0	25.03.24	Policy Management Group