TITLE	DATA DESTRUCTION POLICY
Overview	Trinity College London ('Trinity') is aware of its obligations under the General Data Protection Regulation (GDPR), to retain personal data in a safe and secure manner for as long as necessary and is required by law 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, special tools must be used to securely erase data prior to equipment disposal. This Data Destruction Policy outlines Trinity's approach to fulfilling such obligations and is closely aligned with **Trinity's Data Retention Policy**.
Purpose	This policy has been developed to define the requirements for proper disposal of paper-based and electronic personal data by Trinity.
Scope	• This policy applies to all Trinity employees, temporary and freelance staff, contractors, consultants, suppliers and data processors working for, or on behalf of Trinity ('staff'). • It also applies to personal data held on all Trinity systems, whether hosted on site or in the cloud, on portable storage media or devices or paper.
Policy	**Manual or Paper-based Data Disposal** 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; 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. Within the terms of Trinity's Data **Retention Policy**, 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 Processor contract, as per GDPR requirements; 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** 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; • USB Sticks; 3. Trinity will appoint an appropriate third party to process the act of destruction of this equipment, using approved and recognised industry standard methods; 4. The third party will be required to sign an appropriate Data Processor contract, as per GDPR requirements;
Destruction and Disposal Procedures	When records or data files are identified for disposal, a register of such records needs to be kept. The procedure for the destruction of Confidential or Sensitive Waste on paper, card or microfiche is as follows: 1. All office quality white or coloured paper should be mechanically shredded if the content is in any way sensitive; 2. If waste is disposed by using the shredder, ensure that it is used safely in accordance with its operating instructions, and that waste is shredded in such a way that it cannot be put back together again, and made comprehensible; 3. All other paper can be disposed of in the boxes or bins provided in offices for environmentally-friendly disposal of white non-confidential and non-sensitive paper waste. The procedure for the destruction of Confidential or Sensitive Waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-Rom, DVD and ZIP drive is as follows: 1. Media that are being destroyed because they are showing signs of damage or are obsolete should be physically destroyed by being cut into pieces or other ways prior to disposal;

	2. Where disks, tapes, DVD or CD ROM are being used to supply data to third parties they should, at the very least, be reformatted before the files are saved on to it. The process of saving files to the disk may overwrite areas of the disk; previously used, but this is no guarantee of preventing retrieval of previously stored files. The most effective way to ensure that media are cleaned of all previous data is to use a utility package to perform a 'secure wipe'; 3. Destruction of back-up copies of such data also needs to be dealt with.
Ramifications & Consequences	Trinity is very much aware of its responsibilities towards the personal data within its care, whether in paper-based or electronic format. Trinity is equally aware that failure to properly dispose of such data can have negative ramifications for Trinity, including regulatory investigations, fines and penalties, negative customer perception, reputational damage 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 guidance. Any questions about disposal should be referred to the DPO (dpo@trinitycollege.com) or 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.
Effective Date	May 2018
Date of next review	May 2021

Document Owner and Approval
The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with operational and General Data Protection Regulation (GDPR) requirements.

This policy was approved by Trinity's Executive on 23 May 2018 and is issued on a version-controlled basis under their signature.

Document History				
	Details of Amendments	**Date**	**Owner**	**Approved**
0.1	Policy first drafted	09 May 2018	Compliance Manager	23.05.2018
0.2	Policy updated	20 Feb 2020	Compliance Manager	
0.3				