Data Destruction Procedure

Introduction

Trinity College London (together with its wholly owned subsidiaries, "**Trinity**", "**us**", "**our**" or "**we**") requires everyone to follow this procedure to ensure that when personal data retained by Trinity reaches the end of its retention period, it is disposed of in a manner that ensures Trinity's compliance with the GDPR[1]. The principles of this procedure should also be followed in relation to the destruction of confidential data or commercially sensitive information.

This policy is non-contractual and Trinity reserves the right to amend this procedure without notice.

Scope

This procedure applies to:

- all Trinity employees and workers;
- 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.

It is the responsibility of every employee to familiarise themselves with this procedure and comply with it.

This procedure focuses on the deletion of personal data but the principles of the procedure should also be followed in relation to the deletion of confidential data or commercially sensitive information.

Related Documents

This procedure should be read in conjunction with Trinity's:

- Data Destruction Policy;
- 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.

[1] In this procedure, "**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).

Main Responsibilities

Trinity's Data Protection Officer ("**DPO**") has overall responsibility for the operation of this procedure and is responsible for ensuring that this procedure is reviewed in line with operational and GDPR requirements. All directors, managers (and designated project leaders, where applicable) are responsible for ensuring adherence to this procedure within their teams.

Procedure

Step 1 – Identify the personal data for deletion: Determine the personal data that needs to be deleted. You may need to refer to the Data Retention Schedule in order to identify personal data held by Trinity (either directly or via personal data processors/sub-processors) that has exceeded its retention period. Please contact the DPO if you have any questions relating to this determination.

Where Trinity needs to comply with a legal requirement or a deletion request from a data subject, you may need to refer to the scope of the data deletion request or the legal requirement in order to identify the personal data that needs to be deleted. In such cases, please contact the DPO and/or the Legal Team to ensure Trinity's compliance with the request/requirement. For further information please refer to the Data Subject Request Policy available under the Resources section of the Intranet.

Step 2 – Ensure that you are authorised to delete the personal data identified: Ensure that the personal data you have identified for deletion in Step 1 above can be legally and safely deleted. To do this:

- you should confirm with the Legal Team and with the P&C team that there is no legal reason for retaining the personal data, such as an ongoing litigation that relates to the personal data;

- you should also check with the DPO and with any teams that are likely to use the personal data identified that there are no operational/organisational reasons for retaining the personal data. For example, in certain cases, the Academic Team may wish to retain data for a longer time period in an anonymised form for research purposes;

- you should check with the IT team whether there are any back-ups of the personal data identified for deletion that may also require deletion. Deletion of back-ups is required to ensure that Trinity complies with its legal obligations around the destruction of personal data;

- you should also check with your line manager to ensure that you are authorised to delete the personal data identified.

Where a personal data deletion request has been received from a data subject, you should work with the DPO to ensure that the data deletion request is legitimate, and that the deletion is authorised as there are exceptions to Trinity's legal obligation to comply with personal data deletion requests from data subjects. For further information please refer to the Data Subject Request Policy available under the Resources section of the Intranet.

Step 3 – Securely delete the personal data identified: Destroy the personal data identified in Step 1 above and confirmed for deletion in Step 2 above in such a way that it cannot be recovered and so that no back-ups or copies of such personal data remains held by Trinity.

The procedure for the destruction of personal data on paper, card or microfiche is as follows:

- all office quality white or coloured paper should be mechanically shredded if the content is in any way sensitive; and

- 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.

Where the data involved is not personal data, confidential data or commercially sensitive in any way, 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 personal data on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-Rom, DVD and ZIP drive is as follows:

- contact IT Services in relation to the deletion of personal data from a Trinity device or where a Trinity device is to be disposed or wiped;

- 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;

- 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' and you should contact IT Services to ensure this is correctly done; and

- the destruction of back-up copies of such data also needs to be dealt with and you should contact IT Services to ensure that this is correctly carried out.

Please contact IT Services to ensure the best procedure for the destruction of personal data within digital files, records or databases, including cloud-stored data as each record type may require a different process and each cloud provider may have different protocols for the secure deletion of data. Note that deleting the records visible on your screen may not be sufficient to ensure that the personal data held by Trinity (including back-ups) is destroyed.

Step 4 – Verify that the personal data has been deleted: Ensure that the personal data has been deleted and cannot be recovered. For personal data held on paper, card or microfiche, ensure that the physical destruction of these is such that recovering the personal data is impossible. For personal data held digitally or on electronic media, please contact IT Services to confirm the best way to carry out this verification to ensure that the personal data cannot be recovered.

Step 5 – Document and report the deletion: Maintain a record of the personal data deleted. Include details in your record such as the types of personal data deleted, the number of data records deleted, the process followed, the date and time of deletion and the individuals involved in carrying out the deletion. Provide a copy of this record to the DPO and to your line manager. Update the record of processing activities (**ROPA**) to reflect this deletion of personal data where required by contacting the DPO or during the annual update of the ROPA by all Trinity teams. Consider whether other stakeholders, such as members of the executive, Trinity customers or regulators need to be informed of the completion of the deletion process.

Where personal data has been deleted following on from a data deletion request from a data subject, work with the DPO to ensure that the data subject is informed once the deletion is complete.

Records

Maintain a record of the personal data deleted in accordance with Step 5 of the Procedure above.

Reference Documents

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

Document History				
Version	**Details of Amendments**	**Date**	**Owner**	**Approved**
1	A new procedure created by separating the original Data Destruction Policy into a separate policy and procedure.	25 March 2024	Data Protection Officer	Policy Management Group
2	Change made to the procedure for disposal of devices on IT's request	24 May 2024	Data Protection Officer	