INSTITUTE OF TOURISM STUDIES

DATA RETENTION POLICY

CODE:	P088
OPERATIONAL OWNER:	Data Protection Office
REVIEW DATE:	February 2026
POLICY VERSION:	1.0

Version History

VERSION	DESCRIPTION	AUTHOR	APPROVAL	EFFECTIVE DATE
1	Document Created	DPO	March 2026	6th March 2026
2				

External References

Definitions

Abbreviations

INSTITUTE OF TOURISM STUDIES

Contents

A. Policy and Procedure

Purpose

This Policy sets out the obligations of all the companies forming part of the Institute of Tourism Studies ("ITS") regarding retention of data collected, held, and processed by ITS in accordance with the GDPR, PCI-DSS requirements, and other applicable legal obligations. The purpose of this document is to define the data retention policy for records and documents that are protected or maintained by ITS and to ensure that those which are no longer needed by ITS, or are of no value to ITS, are securely discarded at the correct time. In addition, this policy aids employees of ITS to understand their obligations in retaining paper and electronic documents of all kinds, including word processing documents, spreadsheets, PDFs, emails, pictures, videos, system state data, production data, etc.

This Policy sets out the criteria for determining the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. For further information on other aspects of data protection and compliance with the GDPR, please refer to ITS's Data Protection Policy.

Scope

This Policy applies to all the companies forming part of the Institute of Tourism Studies (hereafter referred to as 'ITS'. This policy applies to all persons within ITS (meaning permanent, fixed term, temporary staff and sub-contractors engaged with ITS). The requirements laid out in this policy must be contractually cascaded to 3rd parties processing, storing, or transmitting ITS data. Adherence to this policy is mandatory and non-compliance could lead to disciplinary or contractual action.

Responsibilities

Asset Owners as assigned in the Asset Inventories have overall responsibility for the management of records and data held within their asset, unless another owner (the Data Owner) has been defined as responsible for the data held within that asset. Such responsibilities ensure that the records created, received and controlled within the purview of their data, and their systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy. The DPO must be involved in any data retention processes and records of all archiving and destruction must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with this policy, a Data Retention Period document (Data Retention Schedule) as maintained by the DPO, the Data Protection Policy and the Data Privacy Program. Data Owners shall be responsible for ensuring that identified retention periods are applied, and determining cases where such data must be retained beyond the identified period. The DPO shall be responsible for reviewing such exemptions prior to approving its retention extension.

Data Retention Guidelines

ITS retains data records efficiently and systematically, in a manner consistent with the GDPR and PCI-DSS requirements. This policy is widely disseminated to ensure a standardized approach to data retention and records management. Records will be retained to provide information about, and evidence of ITS's transactions, customers, employment and activities. After consultation with Legal and Compliance teams, and in accordance with applicable laws, Asset Owners must define retention schedules that govern the periods records must be retained for. These schedules must be documented in a Data Retention Period document (the Data Retention Schedule) or equivalent by the DPO.

All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines. For all data and records obtained, used and stored within ITS, Asset and Data Owners within ITS must apply the following policies and procedures:

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain.
- Establish periodical reviews of data retained.
- Establish and verify retention periods for the data, with special consideration given in the below areas:

  - the requirements of ITS
  - the type of personal data
  - the purpose of processing
  - lawful basis for processing
  - the categories of data subjects

- Where it is not possible to define a statutory or legal retention period as per the GDPR requirement, ITS will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of ITS's standard information disclosures and privacy notices.

- If ITS is served with any legal or regulatory request for records or information, any employee becomes the subject of an audit or investigation or ITS is notified of the commencement of any litigation against ITS, ITS must suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal or regulatory requirement.
- Documents are always retained in a secure location[1], with authorized personnel being the only ones to have access. Once the retention period has elapsed, the documents are reviewed, archived or confidentially destroyed depending on their purpose.
- Once a record or data has reached its designated retention period date, the Asset Owner or the Data Owner should refer to the **Data Retention Schedule** for the action to be taken.

Destruction and Disposal Of Records & Data

Upon the lapse of the retention period, or when it is determined that the supervening circumstances (litigation) which required the extension of the retention period are no longer present, all information classified as "Sensitive" or "Controlled Internal Use" , whether on paper, electronic or other media, must be securely destroyed. This ensures compliance with the Data Protection laws and the duty of confidentiality ITS owes to its employees, clients and customers. ITS is committed to the secure and safe disposal of any confidential waste and information assets in accordance with contractual and legal obligations and that it is done in an ethical and compliant manner.

Physical Records

ITS retains paper-based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential, and compliant manner.

Irrespective of whether office shredding machines, professional shredding services or other means of shredding are used, a cross-cut or more secure method of shredding must be used. Strip-cut shredders are not approved and not recognized as a secure method for paper disposal. It shall be incumbent upon the Asset Owner or Data Owner to ensure that all personal data is destroyed securely and that it is in no way retrievable, using methods provided or approved by Corporate Services.

Electronic & IT Records and Systems

ITS uses numerous systems, computers and technology equipment in the running of its business processes. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal must be handled in an appropriate and secure manner. While

[1] Locations are listed within the data inventories. Data would be tracked through the data inventories by the data owners for appropriate disposal/destruction following the data retention schedule

the decision and accountability to destroy the data when no longer needed lies with the Asset Owner (or when defined, the Data Owner), the process of deleting data and destroying electronic assets is the responsibility of the CTO. The CTO, through proper delegation and with consideration to the data classification, must ensure a proper process is in place to authorize and then carry out the secure deletion of data and/or destruction of assets in a manner that data cannot be reconstructed or inferred.

This process must be fully auditable involving, as applicable, a combination of secure electronic and physical destruction methods. In lieu of destruction, personal data may be anonymized.

For assets holding data classified as “Controlled Internal Use” or “Sensitive”, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for informing the Asset Owner or Data Owner and for updating the Information Asset Register for the asset that has been removed. It is the explicit accountability of the asset owner to liaise with the IT Department to ensure that all relevant data has been sufficiently removed from the IT device before requesting disposal.

Internal Correspondence

Unless otherwise stated in this policy or the Data Retention Schedule, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.e., where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed). Where correspondence or memoranda that do not pertain to any documents having already been assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases.

Right to Erasure

In specific circumstances, data subjects’ have the right to request that their personal data is erased under GDPR, however ITS recognises that this is not an absolute ‘right to be forgotten’. Data Subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent on which the processing is based and where there is no other legal ground for the processing

- When the individual objects to the processing and there is no overriding legitimate grounds for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation

---

It is also considered important to note that this right shall not apply to the extent that processing is necessary:

- For compliance with a legal obligation to which ITS is subject (such as AML/CFT)

- For the establishment, exercise or defence of legal actions / proceedings

For further information on other aspects of data subject rights, please refer to ITS's Data Subject Access Request (DSAR) Procedure as maintained by the DPO.

The DPO must be consulted prior to any personal data being erased under this right.

Compliance

ITS is committed to ensuring the continued compliance with this policy and any associated legislation, and undertake regular audits and monitoring of records, management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

B. Review

The terms of this policy will be reviewed after its first year of operation and regularly thereafter.

C. Document Control

Version	Purpose of Review/ Changes	Date Published	Date of Next Review
1	New Policy		
2			