Data Retention and Destruction Policy

Data Retention
The Civic Theatre retains all important documentation including information pertaining to financial records and contracts for a minimum period of 7 years. All documents are stored in sealed fire proof containers within The Civic Theatre's premises or off-site in a secure storage facility.

This policy fulfils the requirements of the Civic Theatre's chief funding agencies and complies with EU General Data Protection Regulation GDPR and the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

Reasons for Data Retention
The company does not wish to simply adopt a "save everything" approach. That is not practical or cost effective and would place an excessive burden on company and IT Staff to manage the constantly-growing amount of data. Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation.

Data Duplication
As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Retention Requirements
This section sets guidelines for retaining the different types of company data.

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Tax payments will be held for six years.
- Planning data: 7 years.
- Health and Safety: 7 years for records of major accidents and dangerous occurrences.
- Public data: Public data will be retained for 3 years.
- Operational data: Most company data will fall in this category. Operational data will be retained for 5 years.
- Critical data including Tax and VAT: Critical data must be retained for 6 years.
- Confidential data: Confidential data must be retained for 7 years.

The retention periods for employee and HR records were created with regard for the statutory retention periods for HR Data:

Wage information	3 years

Working hours and related information	3 years
Collective redundancy information	3 years
Records of Leave	3 years
Timesheet records	3 years
Sick Leave	3 years
Parental leave records	8 years
Carer's leave	3 years
Employment permit records	5 years or period equal to duration of employment (whichever is longer)
Employee contracts	5 years or period equal to duration of employment (whichever is longer)
Employment records of young persons	3 years
Accident records	10 years
Recruitment records for unsuccessful candidates	6 months to 1 year
Unsolicited Application forms/CVs	1 year
Safety Training Documentation	Ongoing
Training Documentation	Ongoing

Retention of Encrypted Data
If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data Destruction
Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will use data efficiently thereby making data management and data retrieval more cost effective. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered.

Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's management team. The company specifically directs users not to destroy data in violation of this policy.

Destroying data that a user may feel is harmful to himself or herself is particularly forbidden, or destroying data in an attempt to cover up a violation of law or company policy.

Definitions
Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption: The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.