

**BACK UP AND ARCHIVE POLICY**  
**INTRODUCTION**

This policy is designed to:

- To safeguard the data of Attic Theatre Company
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the software employed in the process.

This policy applies to all equipment and data owned and operated by the organisation. Proper backup, storage, archiving and handling of data is necessary for the Company to achieve its objectives efficiently.

### **Definitions**

- Backup - The saving of files onto online and/or offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Archive - The saving of old or unused files onto online and/or offline mass storage media for the purpose of releasing on-line storage room.
- Restore - The process of bringing data back from the offline media and putting it on an online storage system (usually as a result of accidental deletion or corruption of data, system failure, or disaster).

### **Storage and Back Up Schedule**

Local storage: All data is stored on one PC which provides the network for all documentation. This network consists of three main files: Productions, Admin and Archive. All data is saved to the appropriate folder with the date of creation/ modification included in the document title.

Online: Full backups are performed on an ongoing basis using an online (cloud based) mass media storage system. The company is currently using Livedrive a service which provides real-time synchronisation. Dropbox is used as a secondary back up for current activities (Dropbox provides a free service but has restrictions in space).

Hard copy: Hard copy backups are performed on a quarterly basis and burned on to cd/ dvd. Each disc is labelled with the data content and date of backup. The discs are then stored offsite.

Email data is stored in appropriate folders and managed through the online server GSuite. It is also backed up to the local hard drive, online service on a daily basis and to hard copy discs in line with the hard copy schedule.

### **Responsibility**

The General Manager is responsible for the safe storage, scheduling and maintenance of backups. The General Manager shall develop a procedure for testing backups and test the ability to restore data from backups.

### **Archives**

Archives are made at the end of every year in March. Data from the Productions and Admin folder is transferred to the Archive folder where it is no longer in frequent use.

Email data (sent items) are transferred to archive folders and company members' email account data is archived three months after the member has left the company.

### **Recovery**

In the event of accidental deletion or corruption of information, requests for restoration of information will be made to the General Manager.

In the event of a catastrophic system failure, off-site backed up data will be made available within 3 working days of the installation of replacement equipment.

Reviewed March 2017

V Hibbs - General Manager

Ratified by the Board of Trustees