CARE HOUSING ASSOCIATION
IT DATA BACKUP & DISASTER RECOVERY POLICY

1. Purpose

This policy is designed to protect data in the organisation to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

2. Definitions

Backup - The saving of files to offline media storage for the purpose of preventing loss of data in the event of equipment failure or destruction.

Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

3. Backups

Off-site backups: Backups are taken on a daily basis, and this is monitored remotely by Cares outsourced IT contractor. In the event that a backup is not successful, for whatever reason, the contractor will contact the CEO and advise what measures are necessary to ensure a backup is taken, and any remedial work carried out to ensure consistent backups going forward.

The backup is infinite. Therefore, there are weekly, monthly and annual snapshots taken of the data.

4. Restoring data

In the event of a backup being required, a support ticket should be logged with the IT contractor. They will then arrange to either download the data to Cares' server, or email a copy of the restored files (dependant on size). Any data restoration requests must come from the CEO. A copy of this policy is to be shared with the IT contractor to ensure compliance with GDPR 2018.

5. Responsibility

The designated officer responsible for implementation and monitoring of this policy will be the Chief Executive.

6. Equality and Diversity

We are committed to respecting diversity in all aspects of our work and we will not tolerate any form of discrimination.

7. Commitment and Review

Care will formally review this policy every three years.

Last Review Date July 2020