Disaster Recovery Plan

www.clochhousing.org.uk

ClochHA ClochHA

1. POLICY STATEMENT

Cloch Housing Association (CHA hereafter) acknowledges the importance of its ICT systems in the day-to-day running of the business.

CHA recognises the need for and value of a comprehensive ICT Disaster Recovery Plan which aims to minimise risk, disruption and the financial consequences should a disaster occur.

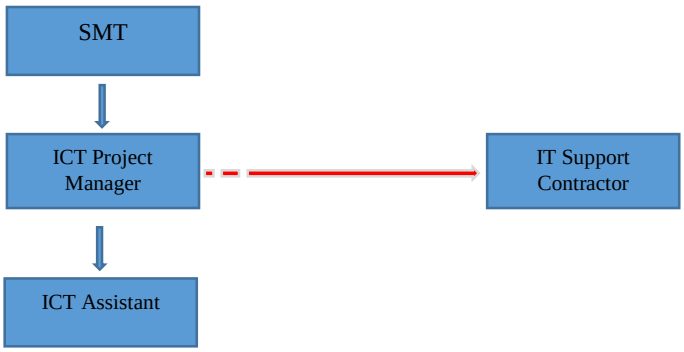
CHA recognises that it is not possible to foresee and anticipate every eventuality, and that some events are out with its control.

2. INTRODUCTION

The IT disaster recovery procedures are to be followed in the event of a disaster concerning the main computer systems at CHA. A disaster will be considered to be a disaster when users are unable to access the central servers and/or data is lost from the system.

Copies of these procedures are to be held by the Senior Management Team (SMT), the IT Project Manager and the IT Support Contractor. Any updates, including updates to contact names and numbers, must be made to all copies and will be carried out by the ICT Project Manager.

CHA's IT support structure is noted below.



3. NETWORK DIAGRAM + COMMUNICATION LINES TOPOGRAPHY

A diagram of Cloch HA's network infrastructure is provided in **Appendix C.**

Details of the current network topology managed by Resource Telecoms is provided in **Appendix D.**

4. TYPES OF DISASTER

The situations below detail the types of incidents that could lead to an ICT disaster:

Environmental Disasters
- Flood
- Snowstorm
- Electrical storms
- Fire
- Subsidence and Landslides
- Freezing Conditions
- Contamination and Environmental Hazards

Organized and / or Deliberate Disruption
- Act of vandalism
- Act of Sabotage
- Theft
- Arson

Loss of Utilities and Services
- Electrical power failure

Equipment or System Failure
- Internal power failure
- Equipment failure (excluding IT hardware)

Serious Information Security Incidents
- Cyber crime
- Loss of records or data
- IT system failure

5. CONTACTS

Listed in TABLE 1 are the contact numbers and addresses for CHA's key personnel, who should be contacted in the event of a disaster:

The personnel below all have the authority to invoke disaster recovery arrangements should a disaster scenario occur, as detailed in Section 4.

TABLE 1

Name	Address	Home Tel	Direct Dial	Mobile
Paul McVey	33 Polbae Crescent, Eaglesham, G76 0LR	01355 301221		07745653590
Alana Durnin	22 Castlepark Drive, Fairlie, KA29 0DF	01475 568861		07947559539
Liz Bowden	Millburn Farm, Millburn Road, Alexandria, G83 0AZ	01389 499872		07943643014
Paul McColgan	364 Carmunnock Road, Glasgow, G44 5BZ	0141 5624643		07753142415
Andy Thompson	11 Orchard Crescent, Port Glasgow, PA14 5DS	01475 741742		07807292045
Ewan Barr	16 Swift Avenue, Inverkip, PA16 0LQ	01475 272806		07921612036

6. ICT SUPPORT CONTACTS

Listed in TABLE 2 are the contact numbers and addresses for the key ICT Support Contractors should a disaster occur:

TABLE 2

Support Provider	Services / Software	Contact Number	Contact Email	Main Contact
Tecnica Ltd	IT Infrastructure / Network Security	01383 722757	support@tecnica-ltd.co.uk	Colin Archer
Resource Telecom	Communication Lines / Phone System / Security Camera's	01355 575111	support@resourcetelecomgroup.com	Stephen Burns / Martyn Wheelans
SDM	Housing Management System / Finance System	01244 301661	helpdeskuk@sdmhousing.co.uk	Scott Drever
Canon	Multifunction Devices / Uniflow	0207 600186	vince_russell@cuk.canon.co.uk	Vince Russell
Sage	Payroll System	0845 111 5555	N/A	N/A
INVU	Document Management	01604 878010	Technical@invu.net	Hugh Bell
ACT	Care and Repair System	0845 268 0220	software.support@swiftpage.com	N/A

7.BACKUP PROCEDURES

Backup procedures are carried out at server level based on CHA's data being held on the servers listed in the TABLE 3 below:

TABLE 3

Main Servers				
Server Name	**Location**	**Manufacturer**	**Model**	**Serial No**
CHA-HV1 (Hypervisor Host)	Cloch HA Office	HP	Proliant DL380 Gen9	CZJ64002N1
CHA-HV2 (Hypervisor Host)	Cloch HA Office	HP	Proliant DL380 Gen9	CZJ64002N3
CHA-DC1	Cloch HA Office	Dell	Poweredge T710	F2BLW4J
CHA-DC2	Cloch HA Office	Virtual	Hyper V	N/A
CHAEX1	Cloch HA Office	Virtual	Hyper V	N/A
CHA-APP1	Cloch HA Office	Virtual	Hyper V	N/A
CHA-SQL1	Cloch HA Office	Virtual	Hyper V	N/A
CHA-RDS1	Cloch HA Office	Virtual	Hyper V	N/A

A full backup of all servers is carried out on the main network as outlined in TABLE 4. Backups are automated and scheduled to run overnight **every** Monday to Friday.

TABLE 4

Server Name	**Main Role**	**Backup Frequency (Daily)**	**Backup Frequency (Weekly)**	**Backup Method**	**Recovery Point Objective (RPO)**
CHA-DC1	Primary Domain Controller	Mon - Thurs (1 Daily Backup) 8 backups retained	Friday (1 Weekly Backup) 52 backups retained	VEEAM backup to disk + site to site replication	1 day for non-hardware related issues
CHA-DC2	Secondary Domain Controller	Mon - Thurs (1 Daily Backup)	Friday (1 Weekly Backup)	VEEAM backup to disk +	1 day for non-hardwar

	+ File Server	8 backups retained	52 backups retained	site to site replication	e related issues
CHAEX1	Exchange Server	Mon - Thurs (1 Daily Backup) 8 backups retained	Friday (1 Weekly Backup) 52 backups retained	VEEAM backup to disk + site to site replication	1 day for non-hardware related issues
CHA-APP1	Application Server	Mon - Thurs (1 Daily Backup) 8 backups retained	Friday (1 Weekly Backup) 52 backups retained	VEEAM backup to disk + site to site replication	1 day for non-hardware related issues
CHA-SQL1	SQL Database Server housing all application DB's	Mon - Thurs (1 Daily Backup) 8 backups retained	Friday (1 Weekly Backup) 52 backups retained	VEEAM backup to disk + site-to-site replication	1 day for non-hardware related issues
CHA-RDS1	Terminal Server	Mon - Thurs (1 Daily Backup) 8 backups retained	Friday (1 Weekly Backup) 52 backups retained	VEEAM backup to disk + site-to-site replication	1 day for non-hardware related issues

The Association backs up all business-critical data using VEEAM as the backup software solution, via the process detailed below.

- Daily backup

  VEEAM software runs a backup to disk at 19:00 daily from Monday to Thursday which includes all servers in the above table. We have the ability to hold the latest 8 daily backups at any one time.

- Weekly backup

VEEAM software runs a backup to disk at 18:00 every Friday which includes all servers in the above table. We have the ability to hold the latest 52 weekly backups at any one time

- Replication

  VEEAM software runs two site-to-site replication jobs daily which includes all virtual machine configuration files and data. One replication is sent to OTHA at 21:00 and the second replication is sent to the IT Support Provider's offices at 23:50. This ensures 2 offsite copies in different locations each day.

Security is maintained by replicating to OTHA and the IT Support Provider's offices over an encrypted IPSEC IKEv2 VPN tunnel. The replicas are secured by the site security including firewalls and up-to-date security patched Hyper-V hosts. VEEAM also encrypts all backups and uses Change Block Tracking (CBT), Microsoft Volume Shadow Copy Services (VSS) and Hyper-V quiescence to maintain the replica integrity.

Before any processing starts in the morning, the previous night's backup must be verified to ensure successful completion. These checks are carried out by the IT Support Provider as part of the support contract and CHA's IT Staff are informed of any major backup fails.

If the backup fails the appropriate action will be taken by the IT Support Provider to rectify the situation.

Backup testing is done every month as part of the support contract activities. CHA's IT staff request a random selection of files to be restored by the IT Support Provider. The restored files are then verified by CHA staff.

Any additional ad-hoc backup that may be required, e.g. prior to version upgrades, are made onto the appropriate media and following completion of the backup, are suitably labelled detailing the date and time of the backup, the person taking the backup, the reason for the backup and any additional relevant information.

Due to the cross-site replication of data and virtual machine configuration CHA's IT systems also allow the facility to restore CHA servers on Oak Tree Housing Association's IT infrastructure. This allows further resiliency when faced with a disaster scenario and allows CHA IT systems to be available more quickly when faced with building damage or hardware failure.

7. RISK ASSESSMENT

a. Risk

The risks outlined in the table on TABLE 5 have been identified and categorised as follows:

Probability: 1 = Low
2 = Medium
3 = High

Impact: 1 = Low
2 = Medium
3 = High

Total: Probability * Impact

Category: 1-3 = Low
4-6 = Medium
7-9 = High

The following ICT risks have been identified and are included in our risk register:

TABLE 5

Risk	Probability	Impact	Total	Category
Server Failure	2	3	6	Medium
Complete loss	1	3	3	Low
Phone System Failure	1	3	3	Low
Website Failure	1	1	1	Low

Our backup procedures detailed in **Section 6** provide steps to manage some the above risks. **Section 8** of this document also specifies the procedures to be followed should any of the above risks develop.

b. Business Critical Systems

This section will define the systems that are critical to the business and also the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for this disaster recovery plan. The RTO is the length of time a business can be without data processing availability and the RPO is how old the data will be once the systems are recovered.

TABLE 6 details the systems that have been defined as critical to business continuity and are those which require restoration within the RTO following a disaster declaration in order to support the restoration of the vital business functions. These software applications and the supporting systems will be recovered within the disaster recovery scenario. The list of business-critical applications and the recovery time and point objectives should be reviewed and updated by the SMT on an annual basis**.**

The following definitions and accompanying table rate the Impact (the amount the business relies on the system) and the System Rating (the importance of the data held on the system) to produce a category rating to calculate RPO and RTO.

Impact: 1 = Low Business functions without item longer term
2 = Medium Business functions without item medium term
3 = High Business cannot function without item

System Rating: 1 = Low Business functions with minimal disruption
2 = Medium System holds valuable but not essential data
3 = High System holds essential business data

Total: Impact * System Rating

Category: 1-3 = Low
4-6 = Medium
7-9 = High

CHA has identified that the following applications are critical to the business and has assessed the risk of failure using the method described above:

TABLE 6

System	Impact	System rating	Total	Category
Housing system (SDM)	3	3	9	High
Telephone System	3	3	9	High
Finance system (SDM)	3	3	9	High
Company file store (Windows File Server)	3	3	9	High
Document Management System (INVU)	2	2	4	Medium
Care and Repair System (ACT!)	2	2	4	Medium
Email access (Exchange Server)	2	2	4	Medium
Network Printing System (Canon Uniflow)	2	1	3	Low
Web access	2	1	3	Low
TimeClock System (Kelio)	1	1	2	Low
Financial Modelling Software (BRIXX)	1	1	2	Low

The RPO and RTO for each risk category is as follows:

Low = 3 working days
Medium = 2 working days
High = 1 working day

The ICT Risk Impact Assessment including a Cyber Risk Assessment can be reviewed for further more in depth analysis of risk.

8. DISASTER RECOVERY SCENARIOS & PROCEDURES

In the event of a major computer disaster being discovered, (see section 4 for disaster examples), the following procedures should be followed in conjunction with the Disaster Recovery Checklist as detailed in **Appendix A**.

Immediately on the discovery of the disaster the following people must be notified using the appropriate contact numbers, as detailed in section 2.

Paul McVey	–	Director
Alana Durnin	–	Finance Director
Andy Thompson	–	Housing Services Manager
Paul McColgan	–	Property Services Manager
Liz Bowden	–	Corporate Services Manager
Ewan Barr	–	ICT Project Manager

In the event of one of staff members being unavailable, then an appropriate alternative from the contact list should be contacted. Having assessed the seriousness of the disaster, the senior person present will contact other personnel as appropriate.

Responsibility for ensuring that the disaster recovery procedures are followed rests with the SMT and the ICT Project Manager, or in their absence the senior staff member present.

If the situation is such that Police and/or Fire personnel are on site, then permission must be obtained from the appropriate authority before entering the site or touching any of the equipment.

Once on site, all equipment within the office must be checked against the Asset Register contained in **Appendix B**. Any missing equipment must be listed.

Virus Intrusion & Related ICT Security Incidents

In the event of a serious virus infection all users should log out of all systems immediately. Should the IT Support Provider be unaware of the intrusion the ICT Project Manager will contact them directly to advise.

The IT Support Provider alongside the organisation will then follow the relevant procedures to investigate and remediate any virus infection or security incident and make systems safe.

Telecommunications

In the event of a complete loss of phone systems or telecommunications lines the ICT Project Manager will contact the Telecommunications Support Provider to instruct them to troubleshoot and restore the phone system. If the problem is out

with the Telecommunication Support Providers control they will escalate to the relevant telecommunications company. The Association has a standalone analogue telephone line for emergency use and staff also have mobile telephones which should continue to be operational should the organisations internal phone system be down.

ICT Hardware & Software

In the event of the Association's main offices, or the hardware within it, being a total loss, the Association will work with the IT Support Provider to restore business critical systems.

Priority will be given to the Housing System and the Finance System with the integrity of the data checked before staff access is granted. Depending on the severity of the issue it may be necessary to contact the relevant software support helpdesk for support and procedures in relation to reinstalling core systems in order to restore the data from backup. The IT Support Provider would assist in locating and setting up alternative servers to restore business critical systems and allow remote access from temporary accommodation.

If the premises are accessible and the server is intact and operational then connections to all clients and printers should be checked. Once this has been completed the server should be switched on and a check of the functionality of programs and data should be made. A fuller more detailed check must be carried out at the earliest opportunity by all users.

No further updating of information is allowed until all users have confirmed that the data in the relevant systems is up to date.

If data is incorrect or has been corrupted in some way, then the most recent available backup is to be used to restore the system to that point. Assistance and procedures to restore from backup can be obtained through the IT Support Provider and the relevant software support provider.

A list of passwords required for reloading systems and for setting up users on the system should be obtained from the ICT Project Manager. The password list is held in the Disaster Recovery folder on an encrypted USB drive within the fireproof safe.

Once the replacement hardware and relevant software have been set up, all users must be notified of the point to which the backup relates e.g. date and time of last entries on the system, at the earliest possible opportunity.

Users must also be requested to confirm that the system is as expected and that they have access to the same programs and data that they had access to prior to the disaster.

No processing should be allowed until all such confirmations are completed.

As soon as the system is available for processing of data **all** passwords must be changed and the system will prompt all users for a new password.

As soon as the above procedures are completed and processing recommences, an insurance claim form must be completed, if appropriate, and submitted to the Insurance Brokers.

At this point the relevant check lists should be double checked to ensure that all procedures have been completed. Once all procedures have been completed the check list must be signed and dated by the Director. A brief report should then be completed and addressed to the Association's Board detailing the problem and the procedures followed to recover from the problem including the extent of any data loss and the impact this may have on service delivery.

A checklist to ensure all procedures have been followed is attached in

Appendix A.

9. STANDING DOWN DISASTER RECOVERY ARRANGEMENTS

Only when the check lists have been double checked and all sections confirmed to be complete then all parties can stand down the disaster recovery arrangements. The Association can then return to a business as usual state.

10. DISASTER RECOVER TESTING PROCEDURE

The purpose of testing the disaster recovery process is to specifically identify and document the task plan and procedures to be implemented in a testing environment. The test plan includes test parameters, objectives, measurement criteria and test methodology to validate the effectiveness of the current disaster recovery procedures. The disaster recovery procedures will be tested to ensure that the Association has the ability to continue the critical business functions in the event of a disaster. It is very important that the recovery procedures are executable and accurate.

Another benefit of testing the plan is to train the personnel who will be responsible for executing the disaster recovery plan. The important issue is not that the test succeeded without problems, but that the test results and problems encountered are reviewed and used to update or revise the current disaster recovery plan procedures. Testing can be accomplished by following the disaster recovery test plan or it may be desirable to execute a subset of the plan. When performing a disaster recovery test, it is very important to use only that information which is recalled from the off-site storage facility. This is to ensure the following:

- Simulate the conditions of an actual disaster recovery situation
- Completeness of the disaster recovery information stored at the retention site
- Ensure the ability to recover the intended functions.

The test plan includes the following areas:

- Schedule
  - Planning Sessions
  - Technical Review

- Introduction
  - Scope
  - Recovery Site
  - Primary Test Objectives
  - Secondary Test Objectives
  - Exclusions
  - Test Assumptions, Dependencies and Success Criteria

- Test Team
  - Identify Project Resources

- Pre-Test Planning
  - Activities
  - Issues
  - Concerns

- Test Timeline
  - Planned start and stop time of test and tasks
  - Actual start and stop time of test and tasks, this step is completed during the test

- Critical Test Checkpoints
  - Activity
  - Recommendation
  - Responsible party

- Test Problem Log
  - Document any problems encountered prior to the test
  - Record any deviations from test plan

The post-test review includes the following areas: -

- Highlights
  - Overall Test Results
  - Test Dates
  - Disaster Recovery Back-up Site
  - Test Participants

- Test Objectives
  - Primary Test Objectives
  - Secondary Test Objectives
  - Exclusions

- Timeline
  - Planned task, start and end times and duration
  - Actual task, start and end times

- Problems Encountered During DR Test
  - Problem Log
  - Actual Problem
  - Target Date for Resolution
  - Status
  - Resolution
  - Problem Summary
  - Follow Up to Pre-Test Problems
  - Follow Up to Suggestions for Improvement/Recommendations from last year's test

- Detailed Summary

- Recommendations

MONITORING AND REVIEW

Monitoring of the IT Disaster Recovery Plan will be undertaken by the Director of Finance and ICT Project Manager. Reporting of any relevant incidents to the Director and Board will occur as necessary.

The IT Disaster Recovery Policy and Plan will be reviewed annually and updated as necessary.

Reviewed by Senior Manager

Signed. . . . . .Date . . . . . .

APPENDIX A

Checklist – Disaster Recovery

	Procedure	**Y/N**	**If N Action**
1.	Have the following personnel been contacted? Director Depute Director ICT Project Manager Finance Director	 **Y/N** **Y/N** **Y/N** **Y/N** **Y/N**	
2.	In the event of structural damage or Police investigations permission must be granted to enter the building. Has permission been granted? Yes – Permission granted by:	**Y/N**	
3.	"Dependent on Scenario" If main office inaccessible, ~~move serve~~r to and notify relevant personnel	**Y/N**	
4.	"Dependent on Scenario" Cable two PC's into ~~server at~~	**Y/N**	
5.	Check equipment against asset list (**Appendix C**)	**Y/N**	
6.	Any missing/ damaged equipment? (If Yes attach list)	**Y/N**	
7.	Check if File Server operational? If YES proceed to '8'. If NO proceed to '6'.	**Y/N**	
8.	Onsite assistance sought from IT Support Provider Ltd for restoring from backup, etc. Housing Management System Helpdesk contacted	**Y/N** **Y/N**	
9.	Replacement server commissioned and remote access tested and working?	**Y/N**	
10.	Check all connections to Servers, PCs & printers. If they are all operational switch on. **Do not input any new data at this stage.**	**Y/N**	

11.	Check set up of users and programs	**Y/N**	
12.	Identify the most recent backup and use to restore data	**Y/N**	
13.	Restore completed & checked	**Y/N**	
14.	Notify all users of the points that the system has been restored to i.e. date, time of last entries etc.	**Y/N**	
15.	Confirmation from all users that access levels and date is as it was before disaster	**Y/N**	
16.	**All** passwords changed	**Y/N**	
17.	Double check the relevant check lists to ensure procedures completed	**Y/N**	
18.	Completed Insurance claim form if necessary	**Y/N**	
19.	Submit claim form to Insurance Brokers	**Y/N**	
20.	Write report to committee detailing the disaster event	**Y/N**	
21.	Report to Management Committee Date: Signed:	**Y/N**	

APPENDIX B

Asset Management Register

ASSET NO.	SERIAL NO.	EQUIPMENT NAME	TYPE	DESCRIPTION OF ASSET (INCLUDING MODEL NO.)
00023	355LV02	ADMIN-PC	PC	DELL Optiplex 3020
0216	R300AVF0	CHA001-PC	PC	LENOVO E50
0233	R300AVCH	CHA010-PC	PC	LENOVO E50
0209	R300CB2T	CHA0112-PC	PC	LENOVO E50
0210	R300CBCK	CHA014-PC	PC	LENOVO E50
0208	R300AVEB	CHA015-PC	PC	LENOVO E50
0212	R300CATE	CHA016-PC	PC	LENOVO E50
0215	R300AVLN	CHA018-PC	PC	LENOVO E50
00022	6MNMF55	CHA021	PC	DELL Optiplex 7010
0221	R300CAR9	CHA021-PC	PC	LENOVO E50
00018	IMNMF55	CHA022	PC	DELL Optiplex 7010
0227	J50Q9X1	CHA028	PC	DELL Optiplex 7010
0287	CZC7087BG9	CHA0287-PC	PC	HP ProDesk 400 G4 MT Business PC
0288	C2C7087B4L	CHA0288-PC	PC	HP ProDesk 400 G4 MT Business PC
0203	3D68D4J	CHA031	PC	DELL Optiplex 960
00019	6T2LV02	CHA032	PC	DELL Optiplex 3020
0211	475LV02	CHA034	PC	DELL Optiplex 3020
00006	IM5LV02	CHA036	PC	DELL Optiplex 3020
0467	CM006682-067	CHA-DSK-0467	PC	ZOOSTORM 7200-2005/A
0201	CM005235-041	CHA-DSK-0201	PC	Zoostorm 7200 6001A
0202	R300AVEE	CHA-DSK-0202	PC	LENOVO E50
0204	CZC435N38	CHA-DSK-0204	PC	HP ProDesk
0205	R300AVCS	CHA-DSK-0205	PC	LENOVO E50
0207	R300AVCY	CHA-DSK-0207	PC	LENOVO E50
0213	R300AVEF	CHA-DSK-0213	PC	LENOVO E50
0214	BX449X1	CHA-DSK-0214	PC	DELL Optiplex 7010
0217	DX459X1	CHA-DSK-0217	PC	DELL Optiplex 7010

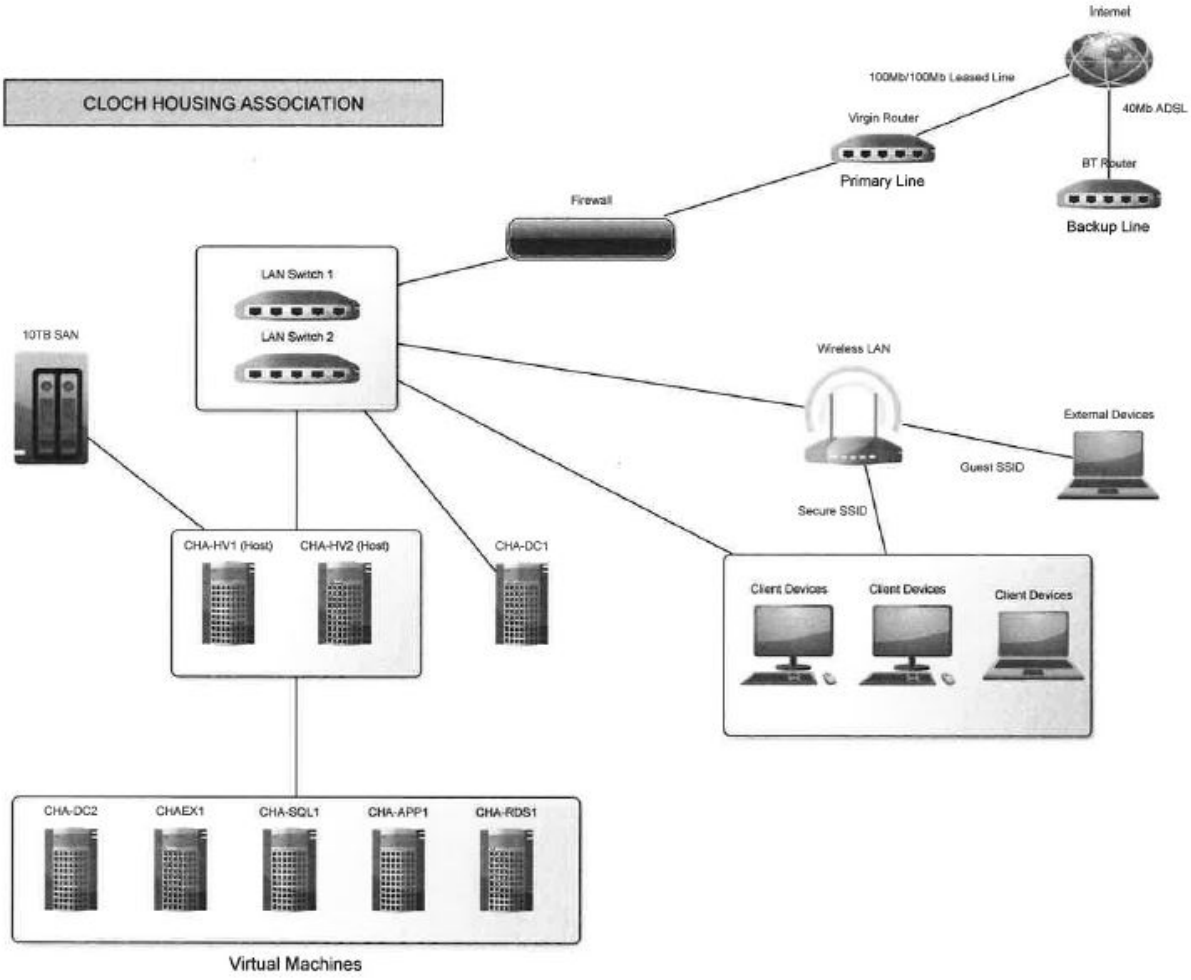
0219	R300CB3N	CHA-DSK-0219	PC	LENOVO E50
0220	BV3K9X1	CHA-DSK-0220	PC	DELL Optiplex 7010
0222	R300AVLT	CHA-DSK-0222	PC	LENOVO E50
0223	JR1N9X1	CHA-DSK-0223	PC	DELL Optiplex 7010
0224	CM005235-023	CHA-DSK-0224	PC	ZOOSTORM
0225	R300AVAK	CHA-DSK-0225	PC	LENOVO E50
0226	R300CAUX	CHA-DSK-0226	PC	LENOVO E50
0228	2SGWY45	CHA-DSK-0228	PC	DELL Optiplex 780
0229	R300AVER	CHA-DSK-0229	PC	LENOVO E50
0230	R300CARF	CHA-DSK-0230	PC	LENOVO E50
0231	R300CATZ	CHA-DSK-0231	PC	LENOVO E50
0234	160Q9X1	CHA-DSK-0234	PC	DELL Optiplex 7010
0235	R300AVEC	CHA-DSK-0235	PC	LENOVO E50
0237	8K5LV02	CHA-DSK-0237	PC	DELL Optiplex 3020
0238	CM019434-003	CHA-DSK-0238	PC	ZOOSTORM
0294	6RPFF4J	CHA-DSK-0294	PC	DELL Optiplex 960
0310	CZC7298P6Z	CHA-DSK-0310	PC	HP ProDesk 400 G4 MT Business PC
0466	CM003701-020	CHA-DSK-0466	PC	ZOOSTORM 7200-2005/A
0480	CZC73176B5	CHA-DSK-0480	PC	HP ProDesk 400 G4 MT Business PC
0232	CFM8WC2	CLOCH100-PC	PC	DELL Optiplex 3040
00021	CFL8WC2	OTHA-DSK-00021	PC	DELL Optiplex 3040
00020	J6562Y1	Lynne-PC	PC	DELL Optiplex 7010
00087	BSK9W4J	OTHA053	PC	DELL Optiplex 780
0295	JKZTWW1	CHA-LAP-0295	Laptop	DELL Latitude E5530
0298	PF-0FX2CP 16/02	CHA-LAP-0298	Laptop	DELL Latitude E560
00001	DNVRQ72	CHALT01	Laptop	DELL Latitude E5570
00002	PF-0FGZLW 16/02	CHALT02	Laptop	Lenovo E560
00005	PF-0FX765 16/02	CHALT05	Laptop	Lenovo E560
01737	F2BLW4J	CHA-DC1	Server	DELL PowerEdge T710
0452	CZJ64002N1	CHA-HV1	Server	HPE Proliant DL380 Gen9 E5-2650v4 2P
0453	CZJ64002N3	CHA-HV2	Server	HPE Proliant DL380 Gen9 E5-

			2650v4 2P
0470	CSTX13 K14888-A11-2320	Server	Fujitsu
0239	CN-0V0VCM-74261-32G-4VMU	Monitor	Dell P2212H
0240	CN-0V0VCM-74261-27Q-1DDU	Monitor	Dell P2212H
0241	CN-0G449H-74445-972-253L	Monitor	Dell 2009WT
0241	CN-091D1V-74445-07F-AHCL	Monitor	Dell 2009WT
0242	CN-0G449H-74445-972-587L	Monitor	Dell 2009WT
0243	CN-0G449H-74445-972-784L	Monitor	Dell 2009WT
0244	CN-0V0VCM-74261-27Q-4VPU	Monitor	Dell P2212H
0245	CN-0G449H-74445-972-283L	Monitor	Dell 2009WT
0246	CN-0G449H-74445-972-779L	Monitor	Dell 2009WT
0247	CN-0646PX-74445-0B1-A275	Monitor	Dell P2011HT
0248	CN-0G449H-74445-972-583L	Monitor	Dell 2009WT
0249	CN-0G449H-74445-972-790L	Monitor	Dell 2009WT
0250	CN-0G449H-74445-972-793L	Monitor	Dell 2009WT
0251	CN-0G449H-74445-972-588L	Monitor	Dell 2009WT
0252	CN-0G449H-74445-792-588L	Monitor	Dell 2009WT
0253	3CQ8200JYY	Monitor	HSTND-2351-F
0254	CN-0G449H-74445-792-591L	Monitor	Dell 2009WT
0254	CN-0G449H-74445-972-591L	Monitor	Dell 2009WT
0255	CN-0G449H-74445-792-785L	Monitor	Dell 2009WT
0256	CN-0G449H-74445-792-589L	Monitor	Dell 2009WT
0257	CN-0V0VCM-74261-32G-4V6U	Monitor	Dell P2212Hb
0258	CN-0V0VCM-74261-32G-4VRU	Monitor	Dell P2212Hb
0259	CN-0V0VCM-74261-32G-4VTU	Monitor	Dell P2212Hb
0260	CN-0G449H-74445-792-247L	Monitor	Dell 2009WT
0261	3CQ8200J2B	Monitor	HP L1908W
0262	ZV0A1619010106	Monitor	Phillips 223V5
0263	CN-0G449H-74445-972-254L	Monitor	Dell 2009WT
0264	CN-0G449H-74448-972-794L	Monitor	Dell 2009WT

0265	CN-0B0BCM-74261-32G4744	Monitor	Dell P2212Hb
0266	CN-0G449H-74445-972-768L	Monitor	Dell 2009WT
0267	CN-0G449H-74445-972-819L	Monitor	Dell 2009WT
0268	CN-0G4494-74445-972-258L	Monitor	Dell 2009WT
0269	CN-0G449H-74445-792-246L	Monitor	Dell 2009WT
0270	CN-0G449H-74445-792-596L	Monitor	Dell 2009WT
0271	CN-0G449H-74445-972-270L	Monitor	Dell 2009WT
0272	CN-0G449H-74445-972-268L	Monitor	Dell 2009WT
0273	CN-0G449H-74445-972-280L	Monitor	Dell 2009WT
0274	CN-0G449H-74445-972-284L	Monitor	Dell 2009WT
0275	CN-0V0VCM-74261-27Q-18WU	Monitor	Dell P2212Hb
0276	Q90063051233	Monitor	ViewSonic VS10866
0277	3CQ8200KMW	Monitor	HP GP536A
0278	3CQ8200JWL	Monitor	HP GP536A
0279	CN-0V0VCM-74261-27Q-1D3U	Monitor	Dell P2212Hb
0280	3CQ8200KQV	Monitor	HP GP536A
0281	3CQ8200K0K	Monitor	HP GP536A
0282	CN-0646PX-74445-0B1-A265	Monitor	HP P2011HT
0283	3CQ8200KY2	Monitor	HP GP536A
0284	3CQ8200L0R	Monitor	HP GP536A
0285	3CQ8200L0Q	Monitor	HP GP536A
0286	0A2JHMBD807625L	Monitor	Samsung S22C150N
0472	HW191DP0REL6Y	Monitor	Hannsg - HSG1033
0477		Monitor	Phillips 223V5
0478		Monitor	Phillips 223V5
0454	FTX2038Y07H	Firewall	Cisco ASA 5512-X NGFW Security Feature Set
0464		Switch	HP 1920-48G (370w) PoE Managed L3 switch
0465		Switch	HP 1920-48G (370w) PoE Managed L3 switch
0455	AS1549143430	UPS	APC (Fujitsu) Smart UPS 1500VA 2U RM LCD

APPENDIX C

Network Diagram



APPENDIX D

Communication Lines

All the below are provided and invoiced by Resource Telecomms who are contracted by both Cloch HA to manage communication lines utilised by the Association.

Cloch HA

Primary Communication Line:

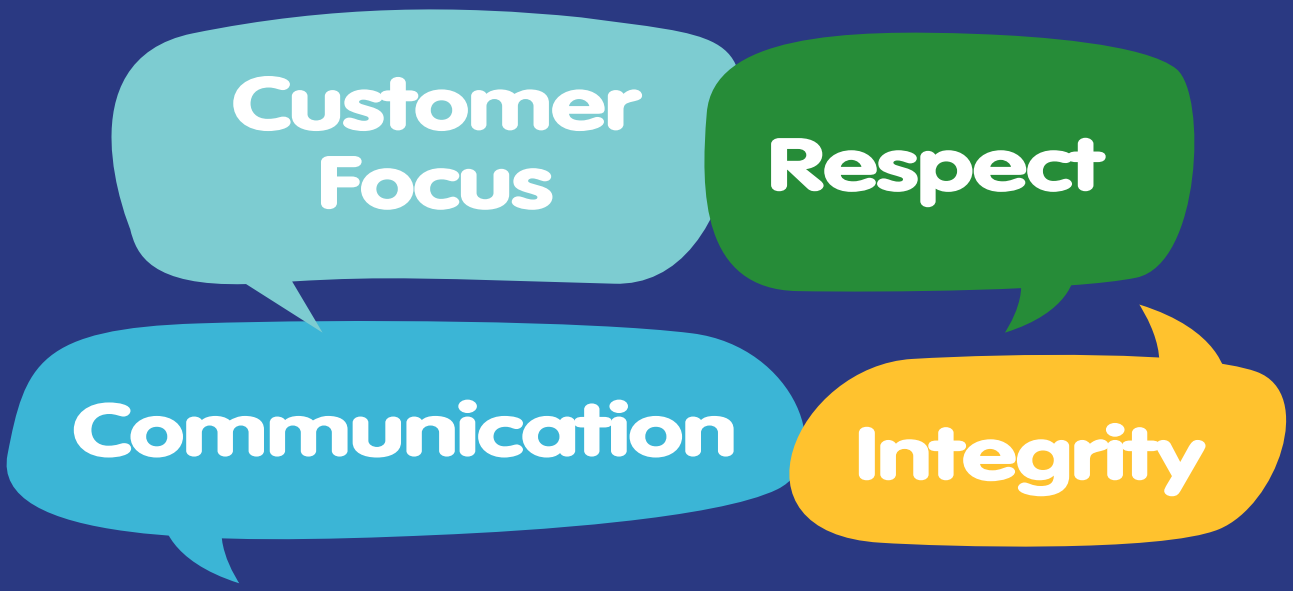
100MB across 1GB bearer Leased Line – provided by Virgin Media via Daisy Communications Datacentre.

Backup Communication Line:

80MB/20MB Fibre To The Cabinet (FTTC) on analogue line 01475 723340 – Provided by BT.

Phone Lines:

8 x Channels of SIP (Session Initiation Protocol) Trunks running on the 100MB Leased Line.



CLOCH HOUSING ASSOCIATION LTD	
Policy Name	Disaster Recovery Plan
Policy Category	HR
Policy Number	065
Date Adopted	20/08/2018
This Review	N/A
Next Review	August 2019
Equalities Impact Assessment Required	
Link to other policies	
Consultation	
Need for Procedure	