



"Offering our community more than a home"

**Draft
CCTV Policy**

Management Committee submission:	25 August 2020
Last Approved:	28 November 2017
Date Approved:	
Next Review date:	August 2023

CHA Objectives:

- To manage the houses provided, in a professional and cost effective manner, for the benefit of our local community and the environment.
- To ensure that our resources are adequate to deliver our objectives by investing in our people, demonstrating value for money and through robust procurement practices.
- To promote social inclusion by applying principles of equality and diversity to everything we do.

Regulatory Standards:

- The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.
- The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these objectives.
- The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.
- The RSL conducts its affairs with honesty and integrity.
- The governing body and senior officers have the skills and knowledge they need to be effective.

Any breach or non-compliance with legislation/regulatory requirements in relation to this Policy constitutes a Notifiable Event and the Regulator will be informed via the SHR Portal.

This policy can be made available on request in a variety of different formats, such as on CD, in large print and translated into other languages.

INDEX

SECTION A

A1	Introduction
A2	Legal Framework
A3	Purpose
A4	Implementation

SECTION B

B1	CCTV Data
B2	Access
B3	Retention and Disposal
B4	Sharing Protocols

SECTION C

C1	Requests
C2	Breach
C3	Complaints

APPENDICES

APPENDIX 1	Sharing Agreement
APPENDIX 2	Data Release Form

CLYDEBANK HOUSING ASSOCIATION LIMITED

A1. INTRODUCTION

Clydebank Housing Association (CHA) is committed to the safety of its staff, tenants and visitors and operates Closed Circuit Television (CCTV) to provide surveillance on a number of its premises.

CCTV is a surveillance system that comprises cameras, recorders and viewing screens. Modern CCTV systems use digital video recorders (DVRs) and digital 'network cameras'. These cameras have higher resolution than previous models, and provide greater flexibility of installation, usage, and in storage of images taken.

Where CCTV is in use, images will be treated as data in the same manner as paper or computer based information.

A2. LEGAL FRAMEWORK

CHA aims to comply with all relevant legislation and guidance on the use of IT equipment but with the following in particular:

- Copyright, Designs and Patents Act 1988
- ~~Data Protection Act 1998~~ the General Data Protection Regulation (EU) 2016/679 ("the GDPR")
- ~~The Freedom of Information Act 1998~~ The Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2019 – applicable from 11 November 2019
- The Human Rights Act 1998
- The Health and Safety at work Act 1974
- Regulation of Investigatory Powers Act 2000
- ~~ICO Privacy and Electronic Communications Regulations~~ the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)
- Environmental Information Regulations

A3. PURPOSE

This Policy has been produced to regulate the management, operation, use and restrictions of the CCTV system. The policy,

- Establishes basic guidelines for appropriate use.
- Sets out the purposes for which it will be used.
- Details the responsibilities and obligations the Association has when using, accessing, storing and sharing data taken from the CCTV system.

- Will be used in conjunction with the police for the prevention and detection of crime.

CHA's CCTV system aims to protect the Association's buildings and assets to safeguard against intrusion, vandalism, damage, disruption and anti-social behaviour.

A4. IMPLEMENTATION OF POLICY

- The Chief Executive ~~is responsible for~~will ensure the implementation and review of this policy.
- The ~~Finance and IT Assistant~~Data Protection and Compliance Officer is responsible for ensuring ~~implementation and that~~ the policy is up-to-date and relevant.
- The Chief Executive and the ~~Finance and IT Assistant~~Data Protection and Compliance Officer are responsible for ensuring all data, images, requests and recordings are managed in accordance with the Association's Data Protection Policy.
- The ~~Finance and IT Assistant~~Data Protection and Compliance Officer is responsible for arranging regular system reviews and to liaise with CCTV maintenance company over any reported faults on the system and updating related procedures.

In the absence of ~~Finance & IT Assistant~~Data Protection and Compliance Officer, all related responsibilities will be covered by the ~~Housing Manager~~Head of Housing Services (in the first instance) and the Chief Executive.

This policy applies to all employees, committee members, agency workers, contractors, and consultants of CHA and therefore all mentioned parties have a responsibility to abide by the principles outlined above and also alert their line manager or ~~Finance & IT Assistant~~Data Protection and Compliance Officer should any behaviours be witnessed which breach this Policy.

Unacceptable behaviour and misuse of any IT equipment as described in the IT Policy will not be tolerated. All breaches of this Policy should be dealt with immediately. Behaviours found to be breaching this Policy will be regarded as misconduct and will be dealt with appropriately and in accordance with the relevant policies, including Code of Conduct and Conditions of Service and the Association's disciplinary procedures *may* be instigated.

B1. CCTV DATA

The main purpose of collecting data from CCTV cameras is the protection of the Association's tenants, residents, service users, employees and the public, the prevention of crime or anti-social behaviour and to safeguard property. Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to other agencies within the scope of our Registration with the Information Commissioner.

Because the information captured by CCTV can be used for crime prevention, CHA must notify the Information Commissioner's Office that it is a data controller and pay the relevant

annual registration fee. The notification includes the purposes for which the images are used, the disclosures that are made and other relevant details.

In applying this policy, all members of staff and committee who have access to images must comply with the Association's Data Protection Policy and ensure that personal information is protected at all times. Users must follow the rules as set out in this policy and relevant procedures, where something is not specifically covered, employees should seek advice from their Department Manager. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the ~~Data Protection Act 1998~~ GDPR and the Association's Data Protection/Management of Information Policy.

Cameras may not always be immediately visible, however signs will be erected to ensure staff, residents and visitors are aware they are entering an area that is covered by CCTV. The signs will include the CHA logo and should:

- be clear, visible and readable
- contain details of the purpose of the surveillance and who to contact about the scheme
- include contact details such as website address, telephone number or e mail address

The Data controller for the Association will monitor the use of CCTV and record the number of instances and details where CCTV images have been requested.

CHA currently have CCTV in the following sites:

- Main Office, 77-83 Kilbowie Road

- Centre 81, 2-16 Braes Avenue
- Castle View, Radnor Park
- Cowal View, Radnor Park
- Erskine View, Radnor Park
- Lennox View, Radnor Park
- Leven View, Radnor Park
- Lomond View, Radnor Park
- Lusset View, Radnor Park

CHA's CCTV systems aim to protect the Association's building and assets to safeguard against intrusion, vandalism, damage, or disruption. The Association's CCTV images will also be used to assist the police in a bid to deter any crime and assist in identifying, apprehending and prosecuting offenders on the Association's property.

Images captured by the system will be monitored in a secure passworded environment on the premises. Password codes will be changed regularly, and should be changed

immediately if they are shared with another staff member for the purposes of an investigation into a serious occurrence.

The Association will operate all CCTV cameras and will check all recording equipment every 12 months.

All images captured by the Association's CCTV systems are digitally recorded. Access to the system is limited to authorised staff and appropriate security measures are in place to prevent external interception. Currently all recorded images are recorded and securely stored on digital video recorders (DVRs).

B2. ACCESS

Access to the CCTV system will be limited to relevant members of staff only.

For operational purposes, and in accordance with the stated purposes of the system, only designated staff, trained in their duties, shall have access to CCTV footage. This access requires two of the listed CHA staff to be present at all times. The following list of these staff is updated as appropriate and should be held by the Data Controller and accessible to Chief Executive:

- Joe Farrell, ~~Housing Manager~~Head of Housing Services (Data Controller)
- Sharon Keenan, Chief Executive
- ~~Michael McLaughlin, Finance & IT Assistant~~Scott Graham, Data Protection and Compliance Officer
- James Inglis, Caretaker
- Charlie Kane, Caretaker
- ~~Donald MacDonald~~John Douglas, Caretaker

All staff members listed above must sign a declaration that access will be for the purposes as stated in clause A3 only.

All access to CCTV data will be recorded in a register which will detail the date, time and reason for access and will be signed by both staff members present.

Except in extremely limited circumstances, the Association must take reasonable steps to let staff know that monitoring in the workplace is happening, what is being monitored and why it is necessary.

Covert monitoring (where the individual is not aware the monitoring is taking place) could only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice. If such monitoring is undertaken it would be advisable to ensure that:

- Management Committee authorises its use;
- it is only carried out for a set timeframe and as part of a specific investigation;
- the risk of intrusion on innocent workers is considered;

- areas where privacy is expected remain private; and
- Limited numbers of people are involved.

B3. RETENTION AND DISPOSAL

CCTV recordings and other materials produced from them shall be retained for one calendar month unless an incident is recorded which requires further investigation. In the latter case, recordings shall be kept for a period of three years from the date of recording.

All media no longer required, on which recordings were made will be returned to the Data Controller to be shredded and the appropriate details entered in the destruction records stored within F:\Systems Admin\Data Protection.

CHA will keep images for at least 28 days, thereafter they will automatically be overwritten from the hard drive of the CCTV systems. Where requested, by the Police or other statutory enforcement agencies, the Association may retain digital images for longer periods until such time as they are able to be viewed by the relevant body – following strict data sharing protocols.

B4. SHARING PROTOCOLS

CHA has written protocols for information sharing with statutory enforcement bodies including Police and Local Authority (Appendix 1). The protocols extend to images that been captured by the Association's CCTV systems and may assist the statutory bodies in the conduct of their duties, including co-operation in live operations where required. Statutory bodies may access images that have been recorded at any time and in accordance with the Sharing agreement for confidential viewing of recorded material stored by the CCTV system

If a statutory enforcement body needs to remove a copy of the recorded material in hard format, they will be required to sign a release form (Appendix 2) detailing:

- The date and time the recorded material was taken
- The date and time range of recorded images and details of which cameras / areas the images are from
- The badge number / name of operative taking the information
- A brief description of why the information is required and for what purposes it will be used
- Once recorded information is transferred to hard format and removed from the control of CHA by a statutory enforcement body, they will become the 'data controllers' as per the Data Protection Act 1998/GDPR requirements and will be responsible for the security and disposal of the information held.

- The Association will retain recorded images for as long as necessary if the information held is subject of a disclosure request (either from a statutory enforcement body or a data subject – member of the public).

C1. REQUESTS

Any images captured of a recognisable person are classed as personal data and are covered by the provisions of the Data Protection Act 1998/GDPR. Anyone that believes they may have been filmed on the Association's CCTV systems has a right to request a copy of this data and the images captured, subject to exemptions contained in the Act.

Data Subjects may make a Subject Access Request (DSAR) for CCTV images/ recordings/ information (request for data about themselves) by applying in writing to the Association and must provide the following information:

- dates and times of the incident with details of the specific location
- photographic proof of identity (e.g. driving licence/passport)
- ~~Cheque or cash in the sum of £10.00.~~

A reasonable charge may be applied if Clydebank HA feel that the DSAR is vexatious or complicated, the charging schedule can be found at:

<https://clydebank-ha.org.uk/uploads/2019-10-28-16-54-50-CHAchargingscheduleSept20-14396.pdf>

A response will be provided promptly and in any event within one month of receiving the required fee and information in accordance with GDPR guidelines. All requests will be detailed within F:\Systems Admin\Data Requests

CHA has the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

C2. BREACH

A copy of this policy will be made available to anyone requesting it. Breaches of this policy should be reported immediately to the Data Controller, Data Protection and Compliance Officer or the Chief Executive. Any complaint concerning misuse of the system will be treated seriously and fully investigated.

Breaches of this policy shall be dealt with in accordance with the appropriate disciplinary policy. Serious breaches of this policy may result in criminal liability on behalf of the individual which may also be considered as gross misconduct.

C3. COMPLAINTS

Any complaints in regard to the operation of the Association's CCTV systems will be dealt with in line with the Association's Complaints [Handling Procedures Policy](#). Complaints can be submitted:

By contacting us on 0141 941 1044
Through the CHA website at <http://www.clydebank-ha.org.uk>
Via email info@clydebank-ha.org.uk
In writing to 77-83 Kilbowie Road, Clydebank, G81 1BL
Or in person to any CHA member of staff

C4. Tenants Use of CCTV and Requests for Installation

If the controller of the CCTV is the tenant then it is the tenants responsibility to ensure it is used correctly, and the only images captured are within the property boundary, under these circumstances the Data Protection Act 2018 does not apply as it is for domestic purposes.

However if the CCTV were to capture images outside the property boundary then the Data Protection Act 2018 would apply to the tenant, and they would need to ensure it was used correctly.

The tenant would be subject to certain conditions found at: <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/>

Therefore If a neighbour was unhappy then they could make a request to the tenant for the CCTV information. A worst case scenario a neighbour could have a case to take action against the tenant under legislation covered by the Human Rights Act. They might have sufficient grounds to say that they have had their privacy violated, that the CCTV system is tantamount to harassment and even voyeurism. In such cases, they may get the police involved.

For Office Use Only – Actions

Customer Consultation Required/Arranged	No
Intranet Update	Yes
F Drive Update	Yes
Website Update	Yes
Leaflet change required?	No
Newsletter Promotion?	No
Other information updated, e.g. posters, automatic email responses, post cards, answering machine messages, etc.	No
Equality Impact Assessment completed	Yes

APPENDIX 1

Clydebank Housing Association

Information Sharing Agreement

This Information Sharing Agreement (ISA) defines the arrangements for processing data between and and sits underneath the overarching Information Sharing Protocol (ISP) / Partnership Agreement. The appendices provide further information and guidance should this be needed.

1. Parties to the agreement: Full name and address of the organisations or businesses

--	--

2. Why is the information being shared?

--

3. What information being shared?

--

4. What is your legal justification for sharing? Has consent been gained if required?

--

5. How will the information be shared? (e.g. data transfer - include any security measures)

--

6. How will the information be stored? (e.g. secure server - include any security measures)

--

7. Who will handle the information – name and job title?

--

8. How long will the information be kept?

9. How will the information be destroyed?

10. What date will the information be shared? Initial date must be later than the date of the signatures below and should give an indication of subsequent dates for regular sharing.

11. What are the names, roles and contact details of any members of staff who will make sure that the required information is shared at the appropriate time?

12. When will this agreement be reviewed and by whom?

This agreement must be formally approved and signed by both parties before any information sharing takes place. Both parties will ensure that the ISA and any associated documents are known and understood by all staff involved in the process.

Originating organisation

Name of organisation:

Name:

Position:

Signature: Date:

Partner organisation

Name of organisation:

Name:

Position:

Signature: Date:

APPENDIX 2

CLYDEBANK HOUSING ASSOCIATION CCTV Request Form

DATA PROTECTION ACT 1998 – Request for disclosure of personal data under s.29(3) of the Data Protection Act 1998

Application to View/Obtain a Copy of CCTV Recording

From:

To: Data Controller, Clydebank Housing Association

Please provide a CD-ROM/DVD copy/still image in respect of the following:

Location(s)	
Date(s)	
Time(s)	
Description of incident/person(s) involved:	
Signed: Name:	Date:
Authorising Signature: Name:	Date: