

CCTV Policy

April 2024

CCTV POLICY

TABLE OF CONTENTS

1	INTRODUCTION	4
2	PURPOSE	5
3	PROTOCOLS	6
4	USE OF AND OBTAINING ACCESS TO CCTV FOOTAGE	7
5	RECEIVING REQUESTS FOR CCTV IMAGES	8
6	RESIDENT REQUESTS TO REVIEW IMAGES	9
7	NEW CCTV INSTALLATIONS	11
8	RESIDENT INSTALLED CCTV	11
9	LEGISLATION	12
10	EQUALITY AND DIVERSITY	12
	ANNEX A - KEY TERMS	12
	APPENDIX 1 POLICE CCTV REQUEST FORM -EXAMPLE	15
	APPENDIX 2 CCTV DATA PROTECTION IMPACT ASSESSMENT	18
	APPENDIX 3 RECORD OF CCTV INSTALLATIONS	22
	APPENDIX 4 CCTV REGISTER OF REQUESTS	26

Impact Assessment

Equality and Diversity - How does the policy adversely or positively impact on anyone under the 9 protected characteristics	No direct impact. All staff receive appropriate Data Protection training (UK GDPR, DPA 2018)
Risk - How does the policy impact on strategic or operational risk or associated controls or assurance?	The policy reduces risk by helping to ensure that all staff are trained on data protection and fully understand the legal position in relation to lawfully processing personal information.
Financial / VfM - What are the financial and VfM impacts?	The introduction of GDPR has led Alpha Living to appoint a consultant to support the organisation through the change process.
Privacy/Data use - Does the policy impact on use of data under GDPR?	This policy outlines the principles of the UK GDPR and DPA 2018 respectively and how data will be used in Alpha Living's day to day business activities.
Health and Safety - Does the policy have any impact on staff or customer health and safety?	No direct implications but will help with identifying more efficient working processes.
Customer impact - What positive or negative impacts will there be for customers or residents?	The policy will help to promote that Alpha Living takes seriously its responsibilities as a landlord and meets its legal and regulatory obligations.

Policy review

All policies will be reviewed every 2 years, or more frequently if required. Policy owners should seek to ensure that all policies are reviewed within the agreed period. Policies which fall outside these timescales will continue to remain in effect until they are formally reviewed. The policy owner should note this may represent a weakness in internal controls.

The Association will operate CCTV in accordance with its Data Protection policy and procedure and will comply with all relevant statutory guidelines and legislation applicable to the Association.

In reviewing this Policy, the Association has taken into account and implemented recommendations from the ICO - “In the picture: A data protection code of practice for surveillance cameras and personal information”.

Overall responsibility for the administration and governance of CCTV remains with the Senior Information Risk Owner (SIRO) supported by the DPO.

INTRODUCTION

- 1.1 This policy sets out how Alpha Living (the association) will manage the collection, retention, processing and management of individuals’ personal identifiable and special category data drawn from the operation of CCTV cameras situated within its BUILDINGS. It is intended to cover the data belonging to our customers, suppliers, employees, workers and other third parties. The policy is designed to incorporate the legal requirements contained in the data protection act 2018, the UK general data protection regulation, (“UK GDPR”) and guidance issued by the information commissioner’s office (“ICO”), in this respect
- 1.2 The association may consider the use of CCTV in the following circumstances:
 1. The prevention and detection of any crime against Association staff or property,
 2. Ensuring public safety,
 3. To protect public and private property,
 4. Monitoring the security of premises and assets,
 5. Working with Police, local authorities and other partnership organisations to identify and take appropriate actions against perpetrators of crime, ASB or breaches of tenancy.

- 1.3 A summary of key terms of attached to this policy at annex A.
- 1.4 This policy is administered by the association's data protection officer, ("DPO"). The DPO will aim to ensure that all staff receive data protection training, including the administration of CCTV UPON starting work with the association and at least once every two years thereafter. This will include how CCTV is deployed and the rules which must be followed for its ongoing administration. Enhanced training will be offered to those members of staff who deal with data to ensure that the policy is up to date and remains relevant to the association and its residents' needs. The policy is owned by the association's SLT and will be reviewed at least every two years.
- 1.5 The association is registered with the ICO under registration number Z7051556.
- 1.6 The following policy and operating principles will apply to all employees and agents of the association. The policy can be provided in any other medium as required by residents to assist them in accessing and understanding their rights in this respect. HR will ensure that a register of training is maintained. The effectiveness of the policy and provision of training will be reviewed annually by the DPO.

2 PURPOSE

- 2.1 This procedure will ensure that the association complies with data protection regulations and protection of freedoms act 2012 (POFA 2012) when creating or processing sound or image records.
- 2.2 The association will comply with the ICO guidance and data protection code of practice for surveillance cameras and personal information and the principles of the surveillance camera code of practice issued by the surveillance commissioner. The association will also have recourse to the data protection act 2018, POFA 2012 and the human rights act 1998.
- 2.3 Article 8 of the european convention on human rights (ECHR) gives individuals the right to respect for their private life, unless interference with this right is necessary for a specified reason, such as preventing crime and protecting the rights and freedoms of others. The convention has been incorporated into UK law by the human rights act 1998.
- 2.4 This policy applies to all personal data collected via the means of CCTV footage regardless of where the media is stored or whether it relates to past or present employees, workers, residents, supplier contacts, or any other data subject. This policy applies to all association employees and must be read, understood and complied with. Compliance with the policy is mandatory and any breach of this policy may result in disciplinary action.
- 2.5 The association recognises that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that the association take seriously at all times.
- 2.6 All individual business areas, departments and supervisors are responsible for ensuring all employees and agents comply with this policy and need to implement appropriate practices, processes, controls and training to ensure compliance.

- 2.7** The DPO is responsible for overseeing this policy.
- 2.8** The DPO should be contacted if there are ever any questions or concerns about the operation of this policy, data protection law in relation to CCTV generally or if there are concerns that the policy is not being followed. In particular, the DPO must always be contacted in the following circumstances:
- ❖ It is not clear under what circumstances the CCTV image request is being made
 - ❖ There are doubts as to the validity of the lawful processing grounds under which the CCTV image is being requested
 - ❖ Advice and guidance are needed

3 PROTOCOLS

- 3.1** All CCTV and image recording will be lawful, fair and transparent and for a specified, explicit and legitimate purpose. Notices will inform data subjects that recording is taking place for all CCTV cameras in situ.
- 3.2** Covert monitoring is rarely justified and should only be done in exceptional circumstances, where openness would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. Covert monitoring will require senior management authorisation and consultation with the DPO.
- 3.3** Recording will be limited to what is adequate and relevant for the purpose.
- 3.4** The simultaneous recording of sound and images will not generally be justified.
- 3.5** Recordings will not be used for any purpose that is not compatible with the purpose for which it was obtained.
- 3.6** Recordings will not be retained for longer than necessary. Generally, recorded images and stills will be kept for a maximum of 28 days from the date of initial download or until investigations are completed or until required for evidential purposes. A retention and deletion document is included as an appendix in the data protection policy.
- 3.7** Recording equipment or systems will allow data subjects to exercise their rights, particularly the right of access to, or deletion of data, where the images relate to them personally.
- 3.8** A data privacy impact assessment (DPIA) will be conducted prior to the introduction of any new recording equipment. (See appendix 1)
- 3.9** All data captured will be stored securely.
- 3.10** Appropriate measures will be taken to prevent unauthorised access or accidental loss of data.
- 3.11** Recording will be for the purpose of crime prevention and detection and for the control of anti-social behaviour (ASB). The CCTV system is intended to provide an increased level of security to make residents', and colleagues, and residents' homes and communities safe and enjoyable places to live and to make our places of work safe for employees.
- 3.12** CCTV images must be clear enough to identify individuals and what they are doing.

- 3.13** Systems will record the minimum necessary to achieve the stated objective, both in terms of the reach of the cameras and the duration of the recording.
- 3.14** In the case of CCTV, a register of systems will be maintained (see appendix 4) the detail of all requests in relation to any request for footage will also be recorded in the CCTV request register (see appendix 3).
- 3.15** Notices will be prominently displayed in areas where CCTV is operating.
- 3.16** Recording equipment will be stored securely and access to recordings will be undertaken by the appropriate association colleague. This will either be the appropriate development manager for the building in which the CCTV request is received. The appropriate person will be determined based upon the circumstances of the request at the time and the availability of colleagues.
- 3.17** Upon receipt of a request the association officer to whom the request is made will check whether the aims and objectives of the request complies with data protection law and will then determine who will check the CCTV for the relevant footage.
- 3.18** Enquiries as to the lawfulness of the request will be made to the DPO or who will assess each request on its merit and will give the go ahead for the search of the CCTV system to see if any positive images exist. If the DPO is not available and the request is urgent, enquiries can be made to the SIRO.
- 3.19** Recordings will be retained for 28 days unless copied as part of criminal or disciplinary proceedings, in which case until such time as the proceedings have been determined.
- 3.20** Disclosures of 3rd party DATA (without the consent of the 3rd party) will be limited to the following:
- Law enforcement agencies or the local authority, where it is believed that the images will assist in a:-
- Legal enquiry;
- Prosecuting agencies.
- 3.21** No other disclosure of 3rd party information obtained via CCTV will be disclosed to requestors unless there is permission from the 3rd party to do so. If a request is received to view CCTV to confirm a positive sighting, access to the system may be made by alpha staff but positive images in relation to a potential image will not be shared directly with a requestor (for example a resident). If the image potentially supports the existence of ASB or an alleged crime, the requestor will be advised to contact the police who may request the footage using the process described at appendix 1 (see paragraph 6.2 below).

4 Use of and obtaining access to CCTV footage

- 4.1 The association will retain a catalogue of CCTV installations within its estates and communities. Any time a camera is installed or decommissioned this log will be updated. The log of requests will be kept by the SIRO. As service charges may be constructed from this information, the DPO will ensure that information in relation to new installations is made available to operational colleagues concerned with the calculation of service charges.
- 4.2 The accuracy of this log is reviewed from time to time in respect of each camera.
- 4.3 Wherever cameras are installed, we will ensure that they are operating lawfully and properly (e.G. Appropriate signs are installed in the relevant places and the cameras are not pointing in inappropriate directions).
- 4.4 Anyone wishing to make a subject access request (SAR) should be asked to complete their request in writing if possible, stating the data they wish to see. All requests should be directed towards the DPO for consideration and action.

5 RECEIVING REQUESTS FOR CCTV IMAGES

Requests for CCTV images are received from several sources but in the case of prevention and detection of crime are likely to derive from the Police. All requests from the Police should be accompanied by an appropriate Schedule 2 Data Protection Act Form, (Appendix 1) which will provide information from the requestor into the circumstances of why images are needed. This should identify the specific lawful processing grounds upon which information can be released if it is available.

Ad Hoc enquiries made by E mail, phone calls, texts from the Police should ensure the request is accompanied by the Schedule 2 disclosure form which will give some written confirmation of the details of the request. Enquiries which do not contain the supporting schedule will be returned to the requester with the attached form for completion.

This gives the Association the evidential credentials it needs to lawfully investigate CCTV systems and forms part of the request recording process in the CCTV Request Register (see Appendix 3).

It is vital that every time CCTV is accessed, the Association record the fact that video footage has been viewed and if appropriate, shared with any 3rd party. Any outcomes of CCTV requests must be communicated via E mail to the DPO. The E mail should contain details of the following

- ❖ Details of the requester (for example which Police Force) the name of the Officer and Crime number if this is available (This should be available on the Request form)
- ❖ Whether any images in relation to the request were available
- ❖ What these images show
- ❖ That the images relate only to the request and show no other data subjects who are not within the scope of the request
- ❖ Whom the images were given to (for example the Police)
- ❖ How the images were given (i.e. transferred by USB or uploaded to a secure site)

6 RESIDENT REQUESTS TO REVIEW IMAGES

- 6.1** Under DPA legislation an image collected under CCTV is classified as personal data and a data subject (e.g. A resident) has limited rights under the act to view footage of themselves. They might under certain circumstances also have the right to have that footage deleted. Generally, a resident might ask to view footage, which relates to their personal circumstances, but which is likely to reveal the identity of a 3rd party. An example might be the viewing of a car collision in a car park for example which damaged their vehicle, or a theft from outside their accommodation.
- 6.2** Under such circumstances it would be permissible for an association officer to view the footage but only for the purpose of establishing if a potential crime has been committed and to then advise the resident whether or not there are images. It will not be possible to show such images to the resident in these circumstances. Only the outcome of the search can be revealed (i.e. There are or there aren't any images) and no other details will be given. If there are images, our policy will be to suggest to the resident that they involve the police who can then request images in line with this policy, for the purposes of investigating an alleged crime.
- 6.3** Requests from residents to view their own images should be referred to the DPO who will advise based on the circumstances of the request at the time.
- 6.4** In order to look at the CCTV, we need to have a lawful basis to do so. The lawful basis we use for viewing **CCTV is under GDPR article 6 (1)(e)** which states: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."
- 6.5** Our CCTV installations are in place for the prevention and detection of crime / ASB so it is only for these reasons we can view the footage. If we are looking for crime / ASB then we can only look at the CCTV if it is proportionate and reasonable to do so.

The proportionality test we will apply having considered the factors at 6.5 are:

- ❖ **Purpose test:** is there a legitimate interest?
- ❖ **Necessity test:** is the processing necessary for that purpose?
- ❖ **Balancing test:** do the individual's interests override the legitimate interest?

- 6.6 We will ask ourselves these questions *every time* the association check the CCTV.
- 6.7 In addition, the association must consider whether checking the CCTV is “strictly necessary”. This means whether the objective the association seek to achieve “cannot reasonably be as effectively achieved BY LESS restrictive of the fundamental freedoms” than viewing the CCTV e.g. What other methods could we use to achieve the same aims?
- 6.8 **This test applies whether the Police ask for the footage or anyone else.**
- 6.9 Any questions about accessing CCTV should be directed to the DPO or any deputy, if there is uncertainty about the lawful processing grounds of the REQUEST.
- 6.10 Processing includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restructure, erasure or destruction.
- 6.11 If the test is satisfied and images are available for viewing, the images should be downloaded and passed to the requester. If the requester is the police, then they should be advised that they will need to have their own USB device onto which they can download any images. The police should provide a receipt for the image so that the association can evidence that data was lawfully passed to the requester.
- 6.12 Releasing images to requestors on association owned USB devices should be avoided.

7 NEW CCTV INSTALLATIONS

- 7.1** The association will carry out a data privacy impact assessment (DPIA) (see appendix 2) prior to installing any new CCTV installations. New installations might arise in response to complaints from residents, the police and employees of incidents of anti-social behaviour, harassment, damage to property and criminal activity.
- 7.2** The DPO should be consulted and will work with the appropriate housing colleagues or stakeholders to determine lawful processing activity for the installation prior to its potential introduction.
- 7.3** In addition to the steps above CCTV recording, monitoring should only take place once the following factors have been considered:
- ❖ The purpose for the monitoring must be in respect of identified and specific criminal activity;
 - ❖ the monitoring must be necessary in order to obtain evidence of that criminal activity;
 - ❖ The covert monitoring should only take place over a specific time period and should not continue after that time period has expired or the investigation has ended;
 - ❖ Any monitoring which is likely to be oppressive must be limited unless there are justified overriding reasons for doing so;
 - ❖ Covert monitoring should not be used in areas where individuals expect privacy such as communal lounges, hallways and workspaces used by employees. (Such as rest rooms) unless there is a real suspicion of serious crime and an intention to involve the police;
 - ❖ Monitoring should be authorised by a Director in consultation with the DPO after appropriate impact assessments have been carried out;
 - ❖ Any information that is not relevant to the main purpose of the covert monitoring (i.e. detecting and preventing criminal activities and unlawful acts) should be disregarded and deleted.

8 RESIDENT INSTALLED CCTV

- 8.1** Permission for residents installing their own CCTV systems for the purpose of providing additional security for their homes is not required, however residents who undertake such installations will be subject to the data protection law applicable to data controllers. The association will make residents aware of these provisions if approaches are made before the installation takes place. A factsheet explaining the main principles is available from the ICO website.
- 8.2** Responses to residents complaining about such installations to the association will advise complainants to make representation to the information commissioner's office (ICO). Residents must seek permission from the association beforehand if the camera is to be fixed to the fabric of the building.

9 LEGISLATION

- 9.1.1 The relevant legislation related to the policy is:
- 9.1.2 Data Protection Act 2018
- 9.1.3 The General Data Protection Regulation EU2016/679.
- 9.1.4 Protection of Freedoms Act 2012 (POFA 2012)
- 9.1.5 Human Rights Act 1998

10 EQUALITY AND DIVERSITY

- 10.1.1 The Association has a specific Equality and Diversity Policy, which reflects not only the legal parameters of the Equality Act 2010 but also embraces the spirit of the Act in recognising the value of diversity in our communities. It reinforces our commitment to eradicating prejudice, discrimination and victimisation in all forms.
- 10.1.2 The Association values diversity and is committed to equal opportunities. We will ensure that this policy is operated fairly and will not discriminate against anyone on the grounds of age, disability, gender identity/reassignment, marital or civil partnership status, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

MONITORING AND REVIEW

- 11.1. The use of the CCTV equipment will be reviewed on at least an annual basis by all relevant personnel mentioned above to ensure that the use complies with legal obligations and this policy. This policy document will be formally reviewed every two years and updated to reflect any changes to corporate/customer requirements and targets.
- 11.2. The association will ensure that any contractors we use to maintain CCTV equipment meet the Information Commissioners standards and requirements.
- 11.3. Any staff found abusing CCTV systems will be subject to disciplinary action in accordance with the Disciplinary Policy and Disciplinary Procedure and may be subject to criminal action.

ANNEX A - KEY TERMS

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR.

We are the Controller of all Personal Data relating to The Association and its employees and Personal Data used in our business for our own professional purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving Processing Personal Data.

Data Protection Officer (DPO): DPOs assist you to monitor internal compliance, inform and advise on the Associations data protection obligations.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU)2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Association

collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Senior Information Risk Owner: The role of a Senior Information Risk Owner is one normally undertaken by a member of an organisation's Senior Management Team. This person takes on overall responsibility for an organisation's information risk policy.

APPENDIX 1 POLICE CCTV REQUEST FORM -EXAMPLE

Request for Information -Schedule 2, section 2 of the Data Protection Act 2018 (DPA) v1

The purpose of this form is to provide justification to support a request for information from third party organisations to the police for the discharge of their statutory functions.

Requester details	
Name of Force	
Contact details of requesting officer	
Date request submitted	
Reference	

Organisation details
Lawful basis for request and disclosure The police have a common law power to exercise powers in relation to a policing purpose which is defined as (a) protecting life and property; (b) preserving order; (c) preventing the commission of offences; (d) bringing offenders to justice; (e) any duty or responsibility of the police arising from common or statute law. The lawful condition for collection of personal data by the police is that the processing is necessary for the performance of a task carried out for a law enforcement purpose (section 35 DPA) and in the case of sensitive processing, that it is strictly necessary for the law enforcement purpose and meets a condition in Schedule 8 DPA. Organisations which have collected personal data for their own purposes are not required to provide fair processing or comply with the purpose limitation principle under Part 2 DPA to the extent that it is necessary for the crime and taxation exemption to apply (Schedule 2, para 2 DPA)

Part 1 - Request for information

Purpose of Request (<i>requesting officer to indicate which purpose applies to the</i>
--

The information is requested for the purpose of:

- ☐ Prevention of criminal activity - there is a substantial suspicion of the threat of criminal activity
- ☐ Detection - there is a substantial suspicion that criminal activity is taking place
- ☐ Investigation - a criminal investigation is ongoing
- ☐ Prosecution - an individual(s) will be charged

Information requested (*requesting officer to specify information sought and justification in relation to the above purpose*)

Information required:

This information is necessary for the above purpose because:

.

Part 2 - Disclosure/Refusal of information

Details of disclosure *(to be completed by disclosing organisation)*
Where information is to be provided by different formats please indicate nature of information to be provided. Where the request is refused please provide reasons, basis for refusal under the DPA'18 and contact details of Data Protection Officer.

-

APPENDIX 2 CCTV DATA PROTECTION IMPACT ASSESSMENT

This assessment is not suitable for assessing the use of covert surveillance, drones, body worn cameras, facial/biometric recognition systems or automatic number plate recognition systems.

We use this assessment tool to satisfy ourselves and the subjects of our CCTV surveillance that we adhere to data privacy legislation and Surveillance Camera code of practice.

The use of CCTV is included in the Data Protection Policy, Privacy notices, CCTV procedure. There are staff training and governance arrangements in place for all data protection issues, including regular reports to leadership and board, a nominated senior responsible officer, and a DPO as single point of contact.

The Association data retention procedure sets out that recordings will be retained for a maximum of 30 days or longer if needed in relation to court action.

Site address	
Surveillance area (e.g., car park, entrance door)	
Number of cameras	
Visible signage in place (Yes/No)	
Server location	
Server security arrangements	
Recording settings (e.g., continuous, motion sensitive, timed)	
Name and contact details of installer/provider	
Does the Installer/provider hold industry specific accreditations? e.g. National Security Inspectorate, British Security Industry Association.	

CCTV is an intrusion into the private lives of individuals and as such consideration should be given to the reasoning, benefits and privacy risks of installing CCTV.

1: Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

- a) What is the problem we face?
- b) What is the lawful basis for use of surveillance?
- c) What is our justification for surveillance being necessary and proportionate?
- d) What alternatives have we considered?
- e) Have we consulted with public and partners to assess if there is a legitimate aim or pressing need for the system?

Answers:

Additional actions required:

2: No more images and information should be stored than that which is strictly required for the stated purpose, and images and information should be deleted once their purposes have been discharged.

- a) How will recordings be deleted at the end of the retention period?
- b) If needed in relation to court action, where will copies of recordings be stored?
- c) How will those copies be deleted following court action?

Answers:

Additional actions required:

3: Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

- a) Who has access to the images and information?
- b) Do we have a written policy on the disclosure of information to a third party?
- c) How do we document decisions about sharing information with third parties?
- d) How do our procedures for disclosure of information guard against cyber security risks?
- e) Do systems allow for privacy masking if any third party is recognisable in images.

Answers:

Additional actions required:

4: Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

- a) What security safeguards are in place?
- b) How do systems guard against cyber security threats?

Answers:

Additional actions required:

5: There should be an effective review and audit mechanism.

- a) How and when will we review the use of CCTV to ensure it remains necessary and proportionate?
- b) What system maintenance arrangements are in place to ensure the ongoing confidentiality, integrity and availability of data?

Answers:

Additional actions required:

6: Quality of images and information of evidential value.

- a) Are the images produced of suitable quality for use as evidence?
- b) Have we involved stakeholders in setting quality standards?
- c) Are there safeguards in place to ensure the forensic integrity of images and information, including a complete audit trail?
- d) Is the information in a format that is easily exportable?
- e) Does the storage ensure the integrity and quality of the original recording?

Answers:

Additional actions required:

--

APPENDIX 3 RECORD OF CCTV INSTALLATIONS

Development	Location of Cameras	Resident Access	What footage can be accessed	Signage	Other information
Alpha Court	1 Main Foyer above office Door, Ground Floor	No	None	Yes	None
	2 Between 2 front entrance doors				
	3 Pointing out to bin yard				
	4 Back Garden, overlooking carpark				
	5 Laundry Camera				
	6 Communal Kitchen				
	7 2nd Floor Corridor between Flats 35 and 36				
	8 Ground floor outside communal toilet pointing towards flat 1				
	2 Entrance				
	3 Entrance				
	4 Entrance				
	5 Ground Floor Corridor				
	6 Ground Floor Corridor				
	7 Lounge				
	8 Lounge				
	9 Car Park (limited View)				

CCTV Policy – Alpha Living 2024

Barnfield	1 Communal lounge/Kitchen Window	No	None	N/K	Situated in main building only. None sited at the Big House or the Lodges
	2 Ground floor corridor near flat 5				Signage required to be erected if not already
	3 Side entrance between flat 12 and 15				
	4 Side Fire Door near flat 22 Fire Door				
	5 Top Floor corridor between Plat 28 and 33				
	6 Outside Car Park adjacent to Flat 23				
	7 Side Entrance outside the laundry				
	8 Fire Door focussing on side garden				
	9 Corridor near the Managers office/Entrance				
Greenside House	1 Front Door, Car Park				Information Needed
	2 RHS building covering grass exits				
	3 LHS building covering grass and lounge area				
Laurence Deacon Court	1 Lobby				Information Needed
	2 Car Park				
	3 Car Park				
	4 Main path into development				
Naseby Court	1 Fire Door Ground Floor				Information Needed
	2 Fire Door Ground floor				
	3 Fire Door Ground Floor				
	4 Main Entrance				
Poppyfields		Information Needed			

Rocklands	1 Main Door				
	2 Covering rear door half way up the drive and side of car Park				
	3 Coverage of other side of Car Park				
St Clements Court		Information Required			
St Peters Court	1 Internal main door				
	2 Dewsbury Road Door				
	3 Ground Floor Foyer				
	4 Communal Lounge Corridor 7-14				
	5 1st Floor				
	6 Corridor 19-25				
	7 2 nd Floor-External				
	8 Main Door Car Park side				
	9 Car Park Bin Area				
	10 Blind corner on side of main building				
	11 Covering up the path along the long block towards the back gate from the linking arch and part of garden seating				
Willow Court	1 Main Entrance Near the lounge				Cameras are focussed on exit doors
	2 Ground Floor near Notice Board				
	3 Lounge near kitchen Door				
	4 Ground Floor Corridor near Flat 7				

Edel Quinn house	No CCTV sited in premises	
Gerard Corr House	No CCTV sited in premises	
Manor House	No CCTV sited in premises	
Oaklands	No CCTV sited in premises	
Regent Court	No CCTV sited in premises	
Saxon Court	No CCTV sited in premises	Said to have no CCTV however do have a camera at the front of the building which is thought to feed into residents flats. Process in place to have this disconnected.
St Columbias Close	No CCTV sited in premises	
The Court	No CCTV sited in premises	
The Mount	No CCTV sited in premises	

APPENDIX 4 CCTV REGISTER OF REQUESTS

Development Description	Date Received	External/internal	Association Officer	Officer (if Police)	Crime Number	Description of alleged crime	Outcome of CCTV Search	Overall Outcome

POLICY REVIEW FORM

Policy Name: CCTV Policy

Review Date: 13/02/24

Lead Reviewer: Jonathan Gladwin (DPO)

Next Review Due: 13/02/2026

Policy Updated on (date):
(date): 4th April 2024

Policy endorsed by SLT / board

Policy communicated to staff through:

On (date):

Lead Reviewers Signature:

A handwritten signature in black ink, appearing to read 'JMG', with a long horizontal line extending to the right.

Jonathan Gladwin

Director of Data Protection Services

TIAA