

CCTV Policy

Date written: 11 July 2018

Date(s) reviewed: July 2021

Last Executive/Board reviewed (approved) date: N/A

Purpose: This Policy identifies the procedures and processes to be followed when planning, implementing and operating a CCTV scheme on Bernicia premises (excluding those properties owned and/or managed by Kingston Property Services and their subsidiaries), and is compliant with the Information Commissioner's Office CCTV Code of Practice (Revised Edition) 2008, data protection legislation, and the Surveillance Camera Code of Practice issued by the Secretary of State pursuant to Section 30 of the Protection of Freedoms Act 2012.

Scope: This policy and supporting guidance confirms how the Bernicia manages its CCTV systems(s), determines who has access to the CCTV data and under what circumstances, including the procedures that will be followed in regard to providing access to CCTV Data.

Definitions:

Associated documents: This document must be read in conjunction with the Information Commissioner's "CCTV Code of Practice" (Revised Edition) 2008, the Surveillance Camera Code of Practice issued by the Secretary of State pursuant to Section 30 of the Protection of Freedoms Act 2012 and Bernicia's Data Protection Policy on Connect and via the following links.

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

Date for review: 31 July 2024

Responsibility: Data Protection Officer

Departments for mandatory read: All Heads of Service and Managers in Housing and PMD

Policy

1. Introduction

- 1.1 Bernicia routinely captures images of people using Closed Circuit Television (CCTV) to provide a safe and secure environment for tenants, colleagues and visitors, and also to protect the company's property.
- 1.2 This policy sets out the accepted use and management of CCTV equipment in line with the Information Commissioner's CCTV Code of Practice to ensure that Bernicia complies with data protection legislation.

2. Policy statements

- 2.1 Closed Circuit Television (CCTV) can be a valuable resource in surveillance and security and is widely used in a range of premises and situations. However, because of the potentially sensitive nature of surveillance, there are codes, guidelines and legislation which must be complied with in order to operate a CCTV scheme legally and fairly.
- 2.2 Bernicia will consider the use of CCTV in order to:
 - deter crime;
 - assist in prevention and detection of crime or Anti-Social Behaviour (ASB);
 - assist with the identification, apprehension and prosecution of offenders i.e. trespassers/burglars;
 - assist with the identification of actions that might result in disciplinary proceedings against colleagues, contractors and tenants;
 - monitor security of property;
 - identify vehicle movement problems around Association properties;
 - to maintain the health and safety of its colleagues/tenants or other lawful purposes;
 - provide reassurance to tenants, so they feel safe and secure.
- 2.3 **Assessment of Need** - Before the installation and use of any CCTV system at a Bernicia property, an assessment of need is to be carried out to determine whether CCTV is justified and if so, how it is to be operated in practice. Issues to be considered in the assessment are:-
 - what is the purpose for using CCTV and what are the problems it is meant to address?
 - what are the benefits to be gained from its use?
 - can CCTV technology realistically deliver these benefits?
 - can less privacy intrusive solutions, such as improved lighting, achieve the same objectives?
 - does Bernicia need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
 - will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

- what future demands may arise for wider use of images and how are they to be addressed?
- what are the views of those who will be under surveillance?
- what could the Association do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?
- how long will the images need to be retained for before destruction?

2.3.1 The assessment of need is to be prepared by the colleague who is recommending the installation of a CCTV at a Bernicia property.

2.3.2 Most CCTV installations will be at Bernicia Housing schemes and the Heads of Housing, Retirement Housing or Assistant Director Care and Support is to authorise their installation, however, any other installation at a property other than a housing scheme is to be authorised by the relevant Director or Chief Executive.

2.3.3 When completed, the signed assessment of need is to be passed to the Data Protection Officer for retention.

2.4 **Covert Recording** - Bernicia is only to undertake covert recording at housing schemes with the written authorisation of the Heads of Housing, Retirement Housing / Assistant Director Care and Support. On the occasions when covert recording is to be used, the Housing Officer responsible for the scheme is to complete the standard CCTV request form (which is to include an assessment of need) and pass it to the Heads of Housing, Retirement Housing or Assistant Director Care and Support for approval. Covert cameras will only be considered where:-

- informing the individual(s) concerned that the recording is taking place would seriously prejudice the reason for making the recording;
- there is good cause to suspect that an illegal or unauthorised action(s) is/are taking place, or about to take place.

2.4.1 Any monitoring is only to be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring (included in the assessment of need), and only for a specific unauthorised activity.

2.4.2 All covert recording activity is to be fully documented, clearly showing who authorised use of the covert monitoring and why.

2.5 **Selecting and Siting Cameras** - CCTV images must be adequate for the purpose for which they are being collected. It is therefore essential to choose the camera equipment and location(s) which achieve the purposes for which CCTV is being used. Cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

2.5.1 Factors to be taken into consideration when siting the camera include:-

- has the camera location been chosen to minimise viewing spaces that are not of relevance to the purposes for which the Association is using CCTV?
- where CCTV has been installed to deal with a specific problem, will the camera be set up so it only records at the time when the problem usually occurs? Alternatively, has consideration been given to other privacy-friendly ways of processing images? For example, some systems only record events that are likely to cause concern, such as movement into a defined area. This can also save on storage capacity;
- will the camera(s) be sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are operating?
- will the camera(s) be suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera?
- will the camera(s) be sited so that they are secure and protected from vandalism?
- will the system produce images of sufficient size, resolution and frames per second?

2.5.2 To judge the quality of images that will be necessary, colleagues will need to take into account the purpose for which CCTV is being used and the level of quality that will be necessary to achieve purpose. Identification of the type of system needed is to be based on the following categories:-

- **Monitoring:** to watch the movement of people where you do not need to pick out individual figures;
- **Detecting:** to detect the presence of a person in an image, without needing to see their face;
- **Recognising:** to recognise somebody who is known to Bernicia, or determine that somebody is not known by Bernicia;
- **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

2.5.3 The type of system required and the quality of images that will be necessary must be included in the assessment of need prepared to justify use of a CCTV system.

2.6 **Installation** - The relevant operational department (Housing, Retirement Housing, Care and Support or Office Services) is responsible for arranging the installation and maintenance of all CCTV systems and must ensure that any installation is carried out by a competent contractor. They must also ensure that :-

- on the date of installation, an initial check of the equipment is to be made to ensure it works properly, they may need to refer to Asset Management for support on this;
- any colleagues required to operate the system/view images, are given sufficient instruction;

- where the time/date is shown on the monitor screen, the information shown is accurate;
- cameras are to be positioned so they will capture images relevant to the purpose(s) for which the scheme has been established;
- the system is set up to carry out constant real-time recording, or only at certain times when suspect activity usually occurs, or is likely to occur (in accordance with the assessment of need);
- a service contract budget is prepared each year (in conjunction with Asset Management and / or Finance as appropriate) to ensure the cameras are maintained by a competent contractor and that a service and maintenance log is kept;
- prominently placed compliant signs are on display to let people know they are in an area where CCTV surveillance is taking place;
- in the event that cameras break down or are damaged, there should be clear system in place so that cameras are restored to working order as soon as possible. All repairs should be reported immediately via the standard repairs system and a log made on the master data base of CCTV (maintained by IT) as to the times and circumstances of the outage;
- where a system is being upgraded or replaced, all details are recorded on the master data base of CCTV, which is held by IT;
- Details of the installation is recorded on the master data base of CCTV administered by IT.

2.7 **Body-Worn Cameras** - Body-worn cameras are an effective tool that can reduce violent confrontations and complaints against colleagues. Body-worn cameras provide additional documentation of encounters between the public and our colleagues, and can be an important tool for collecting evidence and establishing facts.

2.7.1 Bernicia has determined that the use of body-worn cameras can:

- accurately document critical incidents and enhance the accuracy of colleagues testimonies
- provide evidence for investigative and prosecutorial purposes if required

2.7.2 Bernicia recognises that video images cannot always show the full story nor do video images capture an entire scene. The use of body-worn cameras does not reduce the requirement to provide thorough written documentation of an incident. Persons reviewing recordings must also be cautious before conclusions are reached about what the recordings show.

2.7.3 The body-worn cameras should be utilised to:

1. collect evidence that can be used in the prosecution of criminal offenses or in the demonstration of tenancy breaches,
2. protect colleagues who are entering potential violent or dangerous situations and where doing would not place the colleague at increased risk of harm,
3. allow for supervisory review to ensure that appropriate policies and procedures are followed.

2.7.4 Officers must advise that recording is taking place. They shall not edit, alter, erase, duplicate, copy, share, or otherwise distribute in any manner body-worn camera images and information without the prior written approval of the Head of Housing.

2.7.5 All files from body-worn cameras shall be securely downloaded no later than the end of the colleagues working day. Each file shall contain information related to the date, body-worn camera wearer, and the responsible, authorising manager.

2.7.6 All files from body-worn cameras shall be securely stored in accordance with Bernicia's records retention policy and kept for no longer than the retention period set for tenancy files, or for the duration of any active ASBO to which the footage pertains or the duration of a criminal investigation using the imagery.

2.8 **Consulting with Neighbours** - If, for any reason, any neighbouring domestic areas that border the Association's property are included in the camera view, the occupants of the property will be consulted by a Housing Officer/Maintenance Officer prior to any installation. The consultation will be to advise them of the purpose of the CCTV system and how it is being managed and monitored. All details of this consultation must be recorded in the scheme file. Any objections to the installation of a CCTV system are to be dealt with by the relevant Housing Officer/Maintenance Officer.

2.9 **Storing and Viewing Images** – Recorded material is to be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court.

2.9.1 Bernicia will carefully choose the medium on which images are to be stored, and then ensure that access to the images is restricted on a need to know basis. The following should be considered by colleagues when choosing the recording medium:-

- how easy is it to take copies of a recording off the system when asked for by the Police? Can this be done without interrupting the operation of the system?
- will they find your recorded images straightforward to use?
- what will need to be done if recorded material needs to be taken away for further examination?

2.9.2 Viewing CCTV images will be on a strict need-to-know basis. As a general rule images will only be viewed by colleague as follows:-

Independent Living/Supported Housing and Housing with Care Schemes -

- a member of the Senior Management Team;
- a Housing Manager/Assets Manager;
- a Housing Officer/Maintenance Officer;
- a Scheme Coordinator/Housing Support Worker/Tenancy Support worker or Home Manager.

General Needs schemes -

- a Member of the Senior Management Team;
- a Housing Manager/Assets Manager;
- a Housing Officer/Maintenance Officer;

2.9.3 A member of the Senior Management Team can authorise members of s not included above to view images, however, the need to know principle is to be applied at all times.

2.9.4 When viewing images on monitors, colleagues must view them in a controlled room to which employees or others will not have access while the viewing is taking place.

2.9.5 Where images are being viewed remotely i.e. via a broadband link, the same restrictions are to apply.

2.9.6 Where media is removed from a location, the colleague responsible is to record the following information any time media is removed for viewing:-

- date and time the media is removed;
- type of media e.g. disc or pen drive;
- the name of the person removing the media;
- the name(s) of the person(s) viewing the images;
- the name of the organisation to which the person viewing the images belongs;
- the reason for viewing the images;
- the date and time the media is returned.

2.10 **Disclosure** – Bernicia colleagues must ensure that disclosure of images from the CCTV system is controlled at all times and the images taken are consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime, it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated. Where such requests are made an authorised official form (from the organisation requesting the information) must be completed and passed to the Data Protection Officer.

2.10.1 All requests for the disclosure of images to a third party (Subject Access Request) is to be passed to the Data Protection Officer.

2.10.2 The Data Protection Act 2018 give individuals whose images are recorded by the Association have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images.

2.10.3 All Subject Access Requests (SARs) are to be forwarded to the Data Protection Officer who will coordinate all requests for the disclosure of any images held by Bernicia.

2.10.4 Each Subject Access Request is to be acknowledged promptly. Bernicia must respond within one month of receiving the request.

2.10.5 All requests for disclosure will be logged by the Data Protection Officer, however, the collation of images will be carried out by the relevant colleague (for housing properties this will normally be the Housing Officer ASB).

2.10.6 All requests for access to images by individuals (when they are asking for access to images of themselves) should be made in writing to the Data Protection Officer.

2.10.7 Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:-

- The Police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
- prosecution agencies;
- people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);
- colleagues involved with the Group's disciplinary processes;

2.10.8 When making requests for access to CCTV images, applicants are to be asked to provide the following details:-

- the precise date and time when the images were recorded;
- the location of the CCTV camera;
- further information to identify the individual, if necessary;

2.10.9 If Bernicia cannot comply with the request, the reason(s) must be documented and the person who made the request will be advised of these in writing by the Data Protection Officer.

2.11 **Images of Third Parties** - If images of third parties are also shown with the images of the person who has made the access request, s must consider whether to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured.

2.11.1 In many cases, images can be disclosed as there will not be such intrusion, however, is there is any doubt, the Data Protection Officer should be consulted for advice.

2.12 **Retention** - The Data Protection Act does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage.

2.12.1 Images and recording logs will be held in accordance with Bernicia's Data Retention procedures for a maximum period of 28 days

2.12.2 Images stored on removable media such as CDs are to be erased or destroyed once the purpose of the recording is no longer relevant. Confirmation of the destruction of any devices containing images is to be notified to the Data Protection Officer. Any images stored on memory sticks/pen drives should be passed to IT for disposal.

2.12.3 There may be occasions where images may need to be retained for a longer period e.g. where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation. Where this is the case, and images are required to be retained for longer than 28 days, this is to be clearly stated in the assessment of need. Images retained for evidence must be securely stored e.g. in a lockable container e.g. filing cabinet.

2.13 **Register of CCTV** - Assets are to maintain a register of all CCTV installations. The register is to record:-

- scheme
- type of system
- location of hard drive and monitor
- number of cameras
- location of cameras
- confirmation signage is in place
- who has access to the system
- recording length e.g. 7, 14 or 28 days

2.14 **Letting people know** - Bernicia has a duty to let people know that they are in an area where CCTV surveillance is being carried out.

2.14.1 The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV area and reinforcing this with further signs inside the area.

2.14.2 Clear and prominent signs are particularly important where the cameras themselves are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs are to be more prominent and frequent where it would otherwise be less obvious to people that they are on CCTV.

2.14.3 The only occasion when signage will not be displayed, is when covert recording has been authorised by a Director and the display of signage would prejudice its use.

2.14.4 The Assets department is responsible for ensuring that signage is erected at schemes where there are CCTV installations. All signage is to be:-

- clearly visible and readable;
- include the name of Bernicia as the body operating the system, the purpose for using CCTV and who to contact about the

scheme (where these things are not obvious to those being monitored); and

- an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

2.15 **Management Companies** - Where CCTV is in operation within buildings not exclusively owned and managed by Bernicia i.e. those where responsibility lies with a Management Company, Bernicia should ensure that provision is made within Service Level Agreements, that adequate arrangements, which are in line with this policy, are being applied by the relevant Management Company.

2.16 **CCTV Installed by Tenants** - Whilst the Association cannot reasonably withhold permission to allow a tenant to install CCTV installation at their home, the Association must be satisfied that the installation will be used for domestic purposes only. The installation will be treated as an alteration to the property and the tenant will not be permitted to carry out the installation without prior written permission from Bernicia and must be in accordance with the Association's policy on alterations.

2.17 **Complaints** - Complaints and enquiries regarding the operation of the Association's CCTV systems should be addressed to Bernicia's Data Protection Officer.

2.18 **Dummy Signs** – From time to time we may use dummy signs to prevent and deter crime. Where these are in place no images are captured.

3. Responsibility for implementation

3.1 Bernicia is registered on the Public Register of Data Controllers with the registration number ZA329579. The registration must be renewed annually. Failure to notify the Information Commissioner is a criminal offence under data protection legislation.

3.2 There is a requirement that any changes to the Company's registration must be made within 28 days. Failure to notify the Information Commissioner is a criminal offence. If the day-to-day running of the scheme is devolved to someone else, the Data Controller still retains ultimate responsibility for the scheme. The person to whom the running of the scheme is devolved would be committing a criminal offence if they were to act outside the instructions of the Data Controller.

3.3 If the scheme is devolved to a third party such as a Security Company, the advice of the Data Protection Officer must be sought.

3.4 The person responsible for the management of the scheme has a number of responsibilities outlined in this policy. Among these is the need to regularly carry out pro-active checks to ensure that this policy is being complied with, including a review of the on-going value and benefit of the scheme. If the scheme is not achieving its purpose it should be discontinued or modified.

- 3.5 A record of the number and nature of complaints and enquiries must be maintained together with an outline of the action taken in response. A report of these figures must be produced regularly in order to assess public reaction to and opinion of the scheme.

4. Actioning the policy

- 4.1 The designated Manager of the CCTV system must ensure that access to, and disclosure of images recorded by the CCTV system is restricted and carefully controlled and must ensure all employees are aware of the disclosure and access restrictions.

5. Monitoring the policy

- 5.1 Bernicia will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where non-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised.
- 5.2 Disciplinary action may be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits.
- 5.3 The Executive Team will be provided with a summary of audit findings.

6. Resources

- 6.1 This policy should be able to be implemented using existing resources.

7. Equality and Diversity

- 7.1 An equality and diversity impact assessment was undertaken when this policy was originally written. In carrying out our services we are committed to:
- Treating all customers and employees positively regardless of any personal characteristics including gender, age, ethnicity, disability, sexuality, gender reassignment or religion.
 - Taking seriously all complaints and investigating and responding accordingly.
 - Using plain language and providing information in other languages, large print, audio and braille on request.

Uncontrolled if printed – This may not be the latest version of the policy

All policies must be printed from Connect only – please make sure it is the latest version.

Policy Planning Document (PPD)

ALL sections must be completed with a review or any creation of a new, policy. For anything that doesn't apply, please state N/A. Anything left blank will be returned to you.

1. Policy Title*	CCTV Policy
2. Staff/Departments that must be tested*	N/A
3. Staff/Departments for mandatory read*	All Heads of Service and Managers in Housing and PMD
4. Supporting documents, procedures & process maps *	CCTV Form
5. Associated Policies *	Data Protection Policy; Information Complaints Policy
6. Completed E&D Submitted:*	Yes
7. Reason for review (scheduled/non-scheduled)*	Scheduled
8. Minor or Significant change?*	Minor
9. Details of Changes (if any)*	Changed to cover changes in legislation
10. What good practice and ext. learning sources have been used?*	ICO Website
11. Who has been consulted?*	As Above
12. Does this Policy need to go to Board for approval?*	No
13. If any significant change, who has approved this?*	Information Governance Committee
14. Have all legal implications been considered in the policy?*	Yes
15. Does this policy meet regulatory requirements?*	Yes
16. How is the impact of this policy measured?*	Number of CCTV requests received
17. How will training be offered to support these changes?*	Training will be provided / kept up to date for those who access the system.
18. How will the distribution of knowledge be tested?*	N/A
19. Any other information	N/A
Please confirm details below	
Policy Holder	Data Protection Officer
Next Review Date	31 July 2024

Policy Risk and Compliance Assessment

“Policies are documents devised to advise individuals as to a set of behaviours required on a specific topic. Within an organisation they provide a “voice” to the organisation and ensure consistency as well as providing a mechanism for performance management and monitoring.”

As part of reviewing or developing a new policy it is important you complete one of these Policy Risk & Compliance Assessments to tell us a little more about what you are planning so we can support you and your teams appropriately.

Please answer the following questions as honestly and openly as you are able.

This assessment is not to prevent you doing anything, but to centrally offer you the best advice and support in developing and reviewing your policies whilst minimising risk from the outset.

All policies will require this document prior to being hosted on Connect and the review being logged as complete.

Policy Risk & Compliance Assessment	
Name and Job Title	Donna Jackson Information Governance Manager
Department	Risk & Assurance
Title of new policy / policy to be reviewed	CCTV Policy
Brief description of the policy, its purpose, and the areas of the business it covers	<p>This policy identifies the procedures and processes to be followed when planning, implementing and operating a CCTV scheme on Bernicia premises (excluding those properties owned and/or managed by Kingston Property Services and their subsidiaries),</p> <p>This policy and supporting guidance confirms how the Bernicia manages its CCTV systems(s), determines who has access to the CCTV data and under what circumstances, including the procedures that will be followed in regard to providing access to CCTV Data.</p>

Policy Title: CCTV Policy		
Date: June 2021	Name: Donna Jackson	
	Yes	No
1. Equality and Diversity, Will the policy be likely to impact or involve...		
Any individual specifically because of one of their protected characteristics?		√
The collection or processing of information relating to the protected characteristics?	√	
An event or initiative only open to certain people or groups of people?		√
The processing of any information relating to a persons protected characteristics?	√	
The monitoring of a service take up, by protected characteristics?		√
2. Data Protection, Does the policy relate to / involve...		
Collecting data (electronically, with a form or face to face)?	√	
Using, sharing or sending data?	√	
Taking photos?	√	
Sending any information outside of Bernicia?	√	
Asking for any information about children?	√	
Any sensitive information (sexuality, ethnicity, race, religion etc.)?	√	
Technology that will automatically makes decisions or evaluates data?		√
Any systematic monitoring – such as CCTV or tracking?	√	
The large scale processing of data? (there is no definition of large scale, so please use of your discretion in line with Bernicia's business)	√	
Using electronic communications (text, email)?	√	
3. Money Laundering		
Will you be collecting any cash as part of the activity covered in the policy?		√
4. Health and Safety, Will the policy involve...		
Any predominantly any offsite activity?		√
Undertaking an activity with members of the public?		√
Using any PPE?		√
Vehicles (or their use) as a key component?		√
Vulnerable adults, young people or children?		√
Bernicia staff be working on their own or out of hours?		√