

Closed Circuit Television CCTV Group Policy

Responsible Officer

Assistant Director of ICT and Facilities

Aim of the Policy

The aim of this Policy is to set out how we manage and use Closed Circuit Television (CCTV) systems at or around the assets we own or manage.

Cameras are used to monitor activities within buildings and on building sites, including car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of residents, staff, contractors and visitors.

This policy sets out the criteria for the installation and removal of CCTV. CCTV monitoring and recording systems will be installed in or on Phoenix property only when this has been reviewed and approved by the Information Governance Group and relevant Director.

Policy Scope

This Policy and its associated procedures apply to Phoenix and its subsidiaries including all staff whether permanent, temporary or voluntary, Board Members and all contractors working for or on behalf of the Phoenix. It will also apply to residents, regardless of tenure, in terms of how we will respond to requests for personal CCTV in and/or on their own home.

Policy Statement

It is important that all those who are likely to be affected by the use of CCTV cameras, those who are likely to request their use and everyone involved in their operation have a clear understanding of what and how recording will be used.

The key objectives of Phoenix's CCTV system are:

- Detecting and deterring crime and ASB in public areas.
- Assisting in the identification of offenders leading to their arrest and successful prosecution.
- Reducing the fear of crime.
- Ensuring safer neighbourhoods within our communities

Criteria for use

All applications for CCTV whether for fixed, temporary or covert use are required to go through the same 4 stages.

- Application
- Investigation
- Use and management
- Removal

All stages of the process must be followed and the relevant forms retained.

For new build properties, the decision to fit or not fit CCTV cameras will be made during the development process and a Data Protection Impact Assessment be completed.

Application

Applications for CCTV must be made to the Information Governance Group (IGG).

Investigation

The IGG will review the application and consider it against the following set criteria:

- Has a DPIA been completed in full?
- Will using CCTV achieve the set objectives?
- Are there any less intrusive measures that could achieve the same objective (eg extra lighting)
- Is there a clear and demonstrable need for CCTV? (is it proportionate? Is there evidence that supports the need for CCTV?)
- Can the success of these objectives be measured?
- Is the equipment available and the location suitable for CCTV (i.e. is the required infrastructure in place).
- Time: Is there sufficient time to meet the request for the use of cameras? Will S20 requirements apply?
- How will it be paid for? Which budget code will support this work?
- How will the system/cameras be maintained, cleaned, checked?
- Will this be service chargeable to residents?
- Resident consultation.

Once the Group has agreed the application, it will go to the Executive Team for sign off depending on the type of application.

Use and Management

Once an application is signed off it will be passed to the relevant department to process.

For fixed, permanent CCTV, where relevant we will proceed through standard consultation processes including section 20 if necessary. This means the timescales from approval could be up to 12 months.

Temporary, mobile or covert CCTV provision will not be charged to leaseholders unless it has been fitted to address a specific ASB issue such as fly tipping. In these cases, the recharge for leaseholders will be on a pro rata basis so leaseholders are only charged for days the system is on site and in operation.

Once fitted the management of CCTV includes:-

- Management of and access to stored images
- The viewing images by outside agencies
- Access and Disclosure to Individuals Recorded On CCTV
- Destruction of Stored Footage

- Privacy Impact Assessment
- Type of Surveillance
- Data of installation
- Site Checklist
- CCTV equipment in place
- Location of the cameras (register)
- Record of CCTV system quality checks
- Record of CCTV footage requests supplied/denied

Temporary Fixed or Covert cameras

Any proposed request for use must be consistent with the aims and objectives outlined above and should normally cover one or more of the following circumstances:

- Use is requested or supported by the Police
- Use will assist in detection and arrest of perpetrators of a spate of particular crime(s)
- Deployment is to respond to crime hotspots or ongoing ASB problems

Applications must also take the following requirements into consideration:

Justifiable - there must be adequate evidence to show that the cameras are an appropriate and proportionate response. This will usually be shown by evidence of repeated complaints of past incidents, or intelligence on future incidents, evidence from local crime statistics, information shared or received from Community Safety Partnerships, local authorities or events;

General - the target of the surveillance must be in a public area or against unknown offenders.

Reviewable - there must be a clear time limit for the duration of the deployment and an identified process of ongoing evaluation of the need for the cameras' continued use in a specific location. Normal deployments will last approximately 3 months; this may be extended with the agreement of the Director of Operations.

Objective - there must be specified objectives to be achieved by the camera deployment and the achievement of these objectives should be monitored.

Please note that Phoenix will not utilise covert CCTV in private areas such as Extra Care Schemes.

Residents Own cameras

An individual has the right to protect their property and this can be done by using a CCTV system where it is necessary, such as a security measure. However, the Surveillance Camera Commissioner (SCC) recommends that users of CCTV systems should operate them in a responsible way to respect the privacy of others.

A CCTV system to protect a domestic dwelling from acts of crime and anti-social behavior is now commonplace. Although this seems a reasonable use, there have been a number of complaints to the police, ICO and the SCC from neighbours and other members of the public who believe that cameras are being used to spy on them and their families.

If residents are thinking of installing a CCTV system on their home **(including video doorbells)**, they must be made aware of their responsibilities:

- it is their responsibility to make sure that the CCTV system is installed correctly
- they are also responsible for all the information that is recorded by their system
- they must make sure that the information is not used for any other purpose than protecting their property.

If a resident sets up a system so it captures only images within the boundary of their private domestic property (including garden), then the data protection laws will not apply.

However, if the system captures images of people outside the boundary of their private domestic property – for example, in neighbours' homes or gardens, shared spaces, or on a public footpath or a street, then the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) will apply.

Any resident (regardless of tenure) who wishes to attach CCTV to their property must ask and receive written consent before commencing.

Please note that Phoenix will not accept responsibility for the use or management of resident owned CCTV (regardless of whether permission to have CCTV has been granted or not)

Removal

The provision of fixed, permanent cameras will be reviewed on an annual basis to ensure that the need for the cameras remains. If a decision is made that the cameras are not necessary, residents of the block will be informed before removal is allowed. These cameras will be reused on other sites where possible.

Temporary mobile and or covert cameras are allowed to be in place for up to three months. At the end of this period the Information Governance Group will agree that the need to retain these cameras has remained or they will be removed.

In either case, if removal is deemed necessary then this will be completed as soon as is feasible. Where CCTV cameras (fixed or covert) are removed this must be logged accordingly against the [register of CCTV cameras].

Operation for the system

The CCTV operating system will be administered and managed by the Technology and Information Services team in accordance with the principles set in this document.

- Cameras are not monitored on the respective site where they operate routinely, but can be monitored by authorised personnel on devices if staff are on site.
- The CCTV system will be operated 24 hours a day, 365 days of the year.
- Warning signs, as required by the Code of Practice of the Information Commissioner, will be placed at all access routes to areas covered by the CCTV cameras.
- Liaison meetings may be held with all bodies involved in the support of the system.

System control

Access to the CCTV System will be strictly limited to IT, any duty staff and specific authorised persons. Unauthorised persons are not permitted to view live or pre-recorded footage. Personnel authorised to view footage will be declared on the initial application and authorised by the Information Governance Group.

If covert surveillance is planned or has taken place, copies of the written authorisation, including any review or cancellation, must be signed off by Executive Team.

Disclosure of the recorded images to 3rd parties should only be made in limited and prescribed circumstances. If the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Recording is carried out on digital data apparatus. This may be in the form of the camera itself, a locally situated recording device or via a cloud based storage system.

Recorded data will only be released to the media for use to assist the investigation of a specific crime and with the written authority of the police. Recorded data will never be released to the media for purposes of entertainment.

Retention and disposal of material:

- Data disks will be disposed of by a secure method.
- Footage will be stored on data recorder hard drives for a set period of time (no more than 3 months), set and recorded for each device.

Footage will only be stored on data disks if footage is requested by external agencies in the process of detecting crime and in the prosecution of offenders.

Fixed cameras

Fixed cameras will be placed on Phoenix owned buildings permanently (internally & externally) where a need to do so has been identified and the application has been accepted.

No fixed camera will be hidden from view and all will be prevented from focussing on private areas. Signage will be prominently placed at strategic points and at entrance and exit points of the sites to advise residents, visitors and members of the public that a CCTV system is in use. This will display:-

- We are the owner
- The purpose of the CCTV
- Our website and phone number

Although every effort will be made to ensure maximum effectiveness of the system, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

The system will be passively monitored. This means that the CCTV footage is not actively monitored and will only be retrieved following the reporting of an incident.

CCTV images will be only be viewed or accessed by those Phoenix staff identified as having a legitimate reason to do so in the DPIA.

We will hold a CCTV register that covers each site with CCTV in operation. This covers:-

- Property address
- Type of surveillance
- Specific location of CCTV cameras
- The make/model of CCTV camera(s) in use
- The date of installation / date that cameras were in use from and the date that the CCTV camera was removed.
- CCTV use review date
- Reason for CCTV removal
- Location of CCTV DPIA
- Location of where the CCTV footage is stored (locally, The Green Man, cloud)
- Log of any quality checks/maintenance

Legislative & Regulatory Requirements

Regulation of Investigatory Powers Act 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 came into force on October 2000. The Act and accompanying Home Office Guidance is aimed at public authorities charged with the responsibility of identifying individuals and gathering evidence, sometimes against determined criminals. It seeks to regulate what is expected of those public authorities as regards intrusive surveillance.

Phoenix, although not a public authority as defined by the Act, will strive to maintain the relevant standards and to apply good practice.

- Data Protection Act 2018
- GDPR 2016
- Human Rights Act 1998

- Regulator of Social Housing Regulatory Standards
- Protection of Freedoms Act 2012
- Information Commissioner Office – CCTV Code of Guidance
- Home Office - Surveillance Camera Code of Practice

Reference to other documents and associated policies and procedures

- Guidance on use of CCTV and Images provided by residents and other individuals Final V1 2019
- Application for CCTV
- CCTV Register

Definitions

Term/Acroynym	Description
ASB	Anti-social behavior
CCTV	Closed Circuit Television
Directed surveillance	The planned covert surveillance of a specific person if such surveillance is likely to result in the obtaining of private information about that, or any other person would be deemed to be directed surveillance.
DPIA	Data Privacy impact assessments (DPIAs) are a tool we need to use to identify and reduce the privacy risks of individuals (data subjects).
Fixed CCTV	Overt CCTV attached to Phoenix buildings permanently.
Mobile CCTV	Systems set up overtly in areas that do not contain residential Phoenix assets (garage areas, play areas etc. Covert CCTV - surveillance that is carried out without clear identification or signage.
Passive monitoring	When CCTV footage is reviewed after event for specific purposes (i.e. not viewed in real time or live).
SurveillanceCamera Commission	The role of Surveillance Camera Commissioner (SCC) was created under the Protection of Freedoms Act 2012 (PoFA). The SCC was appointed by the Home Secretary and is independent of government. The SCC's statutory functions are to encourage compliance with the Home Secretary's Surveillance Camera Code of Practice.
S20	Section 20 of the Landlord and Tenant Act 1985 which sets out the statutory requirements for consultation with leaseholders and shared owners in major works.
Temporary Fixed	Overt CCTV attached to Phoenix buildings temporarily in response to specific issues (ASB, fly tipping etc.)
ICO	Information Commissioners Officer

Document Type:	Policy
Title:	CCTV Policy
Author	Head of ICT

Department Owned By	ICT & Facilities
Data Protection Impact Assessment	Yes
Equalities Impact Assessment:	No
Approval Date:	28/11/2019
Approved By:	Board
Implementation Date :	29/11/2019
Status:	Final
Version No:	V1
Last updated:	29/11/2019
Issue Date:	10/12/2019
File Path:	